VŠB – Technická univerzita Ostrava
Fakulta strojní
Institut dopravy

Stanovení spolehlivostních charakteristik nové generace modulu automatického vedení vlaku (AVV)

Disertační práce

Studijní program: **P2301 Strojní inženýrství**
Studijní obor: **2301V003 Dopravní technika a technologie**
Školitel: **doc. Ing. Petr Škapa, CSc.**
Doktorand: **Ing. Radek Krzyžanek**

Ostrava 2011

ANOTACE

KRZYŽANEK, Radek. *Stanovení spolehlivostních charakteristik nové generace modulu automatického vedení vlaku (AVV).* Ostrava, 2011. 151 s. Disertační práce. VŠB – Technická univerzita Ostrava, Fakulta strojní, Institut dopravy. Školitel: ŠKAPA, Petr.

Systém automatického vedení vlaku (AVV) je používán pro samočinné řízení hnacích kolejových vozidel a nahrazuje řadu funkcí vykonávaných strojvedoucím vozidla. Pro zajištění bezpečného provozu železniční dopravy je nutné u tohoto systému zaručit vysokou úroveň jeho spolehlivosti.

Tato disertační práce se zabývá problematikou analýzy spolehlivosti modulu UniAVV, který je centrální částí systému automatického vedení vlaku. Hodnocení spolehlivosti je provedeno v souladu s principy funkční bezpečnosti, jež charakterizují požadovanou úroveň spolehlivosti systémů souvisejících s bezpečností pomocí ukazatele úrovně integrity bezpečnosti (SIL).

Disertační práce je tvořena částí teoretickou a experimentální a je rozčleněna do osmi kapitol. Úvodní kapitola teoretické části je věnována popisu funkcí systému automatického vedení vlaku a technického řešení modulu UniAVV a jeho vazeb se zabezpečovacím systémem ETCS. V dalších kapitolách jsou představeny základní principy funkční bezpečnosti elektronických systémů souvisejících s bezpečností a je uvedena teorie provozních a zrychlených zkoušek spolehlivosti.

Experimentální část je věnována určení a ověření skutečné úrovně spolehlivosti modulu UniAVV. Je provedena kvalitativní analýza způsobů a důsledků poruch a kvalitativní hodnocení rizika modulu UniAVV, na jejichž základě jsou v souladu s principy funkční bezpečnosti stanovena opatření ke snížení rizika na přípustnou úroveň. Při kvantitativním hodnocení spolehlivosti modulu UniAVV je vytvořen teoretický model bezporuchovosti, na jehož základě jsou vypočteny ukazatele funkční bezpečnosti, s jejichž využitím je provedeno prokázání dosažené úrovně integrity bezpečnosti. Pro ověření skutečně dosažené úrovně spolehlivosti modulu UniAVV je navržen program provádění zkoušek spolehlivosti a je vytvořen software pro vyhodnocování těchto zkoušek, prováděných v různých režimech jejich realizace.

ANNOTATION

KRZYŽANEK, Radek. *Dependability characteristic assessment of new generation module of automatic train operation (ATO).* Ostrava, 2011. 151 p. Dissertation thesis. VŠB – Technical University of Ostrava, Faculty of Mechanical Engineering, Institute of Transport. Supervisor: ŠKAPA, Petr.

System of automatic train operation (ATO) is used for a self-operated control of power railway vehicles and it replaces number of functions which are realized by an engine driver. For assurance of a safe railway transport operation it is necessary to guarantee the high level of this system dependability.

This dissertation thesis is concerned with the dependability analysis problems of UniAVV module which represents the central part of automatic train operation system. Dependability evaluation is realized pursuant to functional safety principles that characterize demanded level of a safety related system dependability using safety integrity level (SIL) parameter.

Dissertation thesis is composed of theoretical and experimental part and it is divided into eight chapters. The first chapter of theoretical part is devoted to description of automatic train operation functions and technical solution of UniAVV module and its connections to the safety system ETCS. In next chapters there are introduced basic principles of functional safety of electronic safety related systems and theory of operational and accelerated dependability testing is mentioned.

Experimental part is devoted to determination and verification of inherent dependability value of UniAVV module. There are realized qualitative failure mode and effect analysis and qualitative risk evaluation of UniAVV module. On the basis of these analyses there are determined measurements for risk reduction to tolerable level according to functional safety principles. The theoretical reliability model is created as a result of quantitative dependability assessment of UniAVV module. This model is used for calculation of functional safety parameters which are utilized for proof of achieved safety integrity level. The programme of dependability testing is designed for verification of achieved inherent dependability level of UniAVV module. The software is created for evaluation of dependability testing in the different realization modes.

Poděkování

Na tomto místě bych chtěl poděkovat svému školiteli doc. Ing. Petru Škapovi, CSc. za vedení během mého doktorského studia. Zvláštní poděkování patří Ing. Janu Famfulíkovi, Ph.D. a Ing. Janě Míkové, Ph.D. za cenné rady, připomínky, poskytnuté konzultace a jejich trpělivost při vypracování této disertační práce. Rád bych jim také poděkoval za vstřícný přístup a jejich podporu v průběhu mého studia.

OBSAH

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ 7

1 ÚVOD 9

1.1 Stav řešené problematiky 9
1.2 Cíle disertační práce 12

2 FUNKCE, STRUKTURA A VAZBY SYSTÉMU AVV 14

2.1 Základní principy a funkce 14
2.2 Mobilní část systému AVV 18
2.2.1 Modul automatického vedení vlaku UniAVV 19
2.3 Traťová část systému AVV 21
2.3.1 Informace o poloze vozidla 21
2.3.2 Informace ze zabezpečovacího systému 23

3 ANALÝZA SPOLEHLIVOSTI S VYUŽITÍM PRINCIPŮ FUNKČNÍ BEZPEČNOSTI 25

3.1 Základní principy 25
3.1.1 Životní cyklus celkové bezpečnosti 26
3.1.2 Úroveň integrity bezpečnosti 28
3.2 Kvalitativní hodnocení funkční bezpečnosti 31
3.2.1 Metoda ALARP 32
3.2.2 Diagram rizika 33
3.3 Kvantitativní hodnocení funkční bezpečnosti 35
3.3.1 Diagnostické pokrytí 36
3.3.2 Cílová míra poruch 38

4 ZKOUŠKY SPOLEHLIVOSTI 43

4.1 Provozní zkoušky spolehlivosti 43
4.1.1 Zkušební plány 43
4.2 Zrychlené zkoušky spolehlivosti 47
4.2.1 Arrheniův model 49
4.2.2 Teoretický model pro zrychlené zkoušky systémů 50

5 KVALITATIVNÍ ANALÝZA SPOLEHLIVOSTI MODULU UniAVV 56

5.1 Analýza způsobů a důsledků poruch (FMEA) 56
5.1.1 Kritéria provedení analýzy 57
5.1.2 Počáteční analýza FMEA 59
5.2 Stanovení požadavků na redukci rizika 67
5.2.1 Určení integrity bezpečnosti modulu UniAVV 67
5.2.2 Omezení architektury hardware 72
5.3 Hodnocení výsledků kvalitativní analýzy spolehlivosti 74

6 KVANTITATIVNÍ HODNOCENÍ SPOLEHLIVOSTI MODULU UniAVV 80

6.1 Teoretický model spolehlivosti – systém AVV 80
6.2 Teoretický model spolehlivosti – modul UniAVV 89
6.3 Hodnocení funkční bezpečnosti modulu UniAVV 92
6.3.1 Určení diagnostického pokrytí 95
6.3.2 Určení cílové míry poruch 100
6.3.3 Zhodnocení dosažených výsledků 102

7 NÁVRH PROGRAMU ZKOUŠEK SPOLEHLIVOSTI PRO MODUL UniAVV . 105

7.1 Provozní zkouška spolehlivosti snímače MIB 105
7.2 Zrychlené zkoušky spolehlivosti bloku logiky 112
7.2.1 Vyhodnocení zkoušky při znalosti aktivačních energií 114
7.2.2 Vyhodnocení zkoušky bez znalosti aktivačních energií 118
7.2.3 Řešení software vyhodnocovacích formulářů 122
7.2.4 Vyhodnocení ověřovací zkoušky 126

8 ZÁVĚR 129

8.1 Přínosy práce pro vědu a praxi 130
8.2 Možnosti dalšího rozvoje problematiky 132

SEZNAM POUŽITÉ LITERATURY 133

SEZNAM VLASTNÍCH PUBLIKACÍ DOKTORANDA 135

SEZNAM OBRÁZKŮ 136

SEZNAM TABULEK 138

PŘÍLOHY

Příloha č. 1: Popis elektrické lokomotivy řady 380 ČD (109 E) 139
Příloha č. 2: Predikce bezporuchovosti elektronických součástek 143
Příloha č. 3: Intenzity poruch součástek bloku logiky modulu UniAVV 148
Příloha č. 4: Hodnocení provozní spolehlivosti snímačů MIB 150
Conclusions 151

CD-ROM

Příloha č. 5: Formulář pro vyhodnocení zkoušek spolehlivosti „Arrhenius 1“
Příloha č. 6: Formulář pro vyhodnocení zkoušek spolehlivosti „Arrhenius 2“

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

ATO	Automatic Train Operation
AVV	automatické vedení vlaku
CAN	datová sběrnice (Controller Area Network)
CB	cílové brzdění
CPU	procesor (Central Processing Unit)
CRC	centrální řídící člen
CRV	centrální regulátor vozidla
ČD	České dráhy, a.s.
DC	diagnostické pokrytí (Diagnostic Coverage)
E/E/PES	elektrický/elektronický/programovatelný elektronický systém
EDB	elektrodynamická brzda
ERTMS	Evropský systém řízení železniční dopravy (European Rail Traffic Management System)
ETCS	Evropský vlakový zabezpečovací systém (European Train Control System)
EUC	řízené zařízení (Equipment Under Control)
FMEA	analýza způsobů a důsledků poruch (Failure Mode and Effect Analysis)
FTA	analýza stromu poruch (Failure Tree Analysis)
LVZ	liniový vlakový zabezpečovač
MIB	magnetický informační bod
OJV	optimalizace jízdy vlaku
RAM	paměť s přímým přístupem (Random Access Memory)
RBD	blokový diagram bezporuchovosti (Reliability Block Diagram)
RCB	regulátor cílového brzdění
RJD	regulátor jízdní doby
RPN	hodnota závažnosti rizika (Risk Priority Number)
RR	regulátor rychlosti
SFF	podíl bezpečných poruch (Safe Failure Fraction)
SIL	úroveň integrity bezpečnosti (Safety Integrity Level)
STM	specifický přenosový modul (Specific Transmission Module)
VTCU	vozidlový počítač
A	zvýšené zatížení
A_F	faktor zrychlení [-]
AND	konjunkce (logický součin)
C	konfidenční úroveň [-]
C	následek nebezpečné události
CD	odhalitelnost poruchy
CO	četnost vzniku poruchy
$E(T)$	střední hodnota náhodné veličiny [h]
E_A	aktivační energie [eV]
ES	závažnost důsledku poruchy
f	četnost výskytu nebezpečné události
F_S	pravděpodobnost poruchy systému [-]
$F(t)$	distribuční funkce náhodné veličiny [-]

$G(T)$	rychlost reakce
H	Hammingův odstup
K	Boltzmanova konstanta ($8{,}617385.10^{-5}$ eV.K^{-1})
$L(T)$	kvantitativní ukazatel spolehlivosti [h]
M	výrobky se během zkoušky opravují
n	počet výrobků zařazených do zkoušky spolehlivosti [-]
OR	disjunkce (logický součet)
PFD	pravděpodobnost nebezpečné poruchy [-]
PFH	cílová míra poruch
r	počet poruch během zkoušky spolehlivosti [-]
R	riziko systémů souvisejících s bezpečností [-]
R	výrobky se během zkoušky nahrazují
R_S	pravděpodobnost bezporuchového stavu systému [-]
t	hodnota náhodné veličiny T [h]
t_{AKU}	akumulovaná pracovní doba zkoušky [h]
t_{CE}	ekvivalentní doba prostoje kanálu [h]
t_{LT}	stanovená životnost systému souvisejícího s bezpečností [h]
t_{PT}	interval mezi diagnostickými testy nebo kontrolními zkouškami [h]
T	absolutní teplota [K]
T_D	dolní mez konfidenčního intervalu [h]
T_H	horní mez konfidenčního intervalu [h]
U	provozní zatížení
U	výrobky se během zkoušky nenahrazují
α	hladina významnosti [-]
χ^2	hodnota chí-kvadrát rozdělení [-]
λ	parametr exponenciálního rozdělení pravděpodobnosti [h^{-1}]
λ_D	intenzita nebezpečných poruch [h^{-1}]
λ_{DD}	intenzita nebezpečných diagnostikovaných poruch [h^{-1}]
λ_{DU}	intenzita nebezpečných nediagnostikovaných poruch [h^{-1}]
λ_S	intenzita bezpečných poruch [h^{-1}]
ν	počet stupňů volnosti rozdělení chí-kvadrát [-]
θ	parametr náhodné veličiny
τ	doba trvání zkoušky [h]

1 ÚVOD

Výkon funkce strojvedoucího je při řízení hnacího kolejového vozidla spojen s vysokými požadavky potřebnými pro zajištění bezpečnosti jízdy vlaku, zejména v oblasti koncentrace a rychlosti reakce. Se zvyšující se rychlostí jízdy vlaků se zvyšuje četnost vjemů působících na strojvedoucího a zároveň klesá doba vymezená pro jeho reakci. Aplikací automatických systémů pro samočinné řízení kolejových vozidel, ať ve formě systému automatické regulace rychlosti, nebo komplexního systému automatického vedení vlaku, dochází ke snížení pracovního zatížení strojvedoucího a tím ke zlepšení jeho pracovních podmínek.

Automatické systémy pro řízení kolejových vozidel nahrazují do značné míry funkce, které jsou vykonávány při manuálním řízení strojvedoucím. Pro zachování vysoké kvality a bezpečnosti jízdy vlaku je nezbytné, aby tyto systémy splňovaly požadavky nejen z hlediska funkčního a technického řešení, ale také z hlediska úrovně jejich spolehlivosti. Systémy automatického řízení vozidel tak musí dosáhnout takové spolehlivosti, která zajistí bezpečný provoz železniční dopravy, a jejich případná selhání vedou pouze k nízkému, společensky přijatelnému riziku.

Nová generace systému automatického vedení vlaku, používaná pro samočinné řízení vozidel v České republice, umožňuje také aktivní spolupráci se systémem jednotného evropského zabezpečovacího systému železniční dopravy (ETCS). Díky maximální interoperabilitě tohoto systému je možné využít systém automatického vedení vlaku pro řízení vozidel i na tratích ostatních států Evropské unie. V této souvislosti je výhodné pro prokázání dosažené úrovně spolehlivosti systému automatického vedení vlaku využít standardizovaný postup, umožňující konzistentní přístup, jež přispívá ke zvýšení konkurenceschopnosti tohoto produktu.

1.1 Stav řešené problematiky

Existuje řada národních a mezinárodních standardů, které definují požadavky spolehlivosti a bezpečnosti technických systémů obecně, i systémů v železniční dopravě.

Základním standardem specifikujícím požadavky spolehlivosti aplikací v železniční dopravě je norma ČSN EN 50126 Drážní zařízení – Stanovení a prokázání bezporuchovosti,

pohotovosti, udržovatelnosti a bezpečnosti (RAMS). Norma definuje proces řízení parametrů RAMS obecně pro drážní zařízení na všech úrovních, avšak neuvádí konkrétní číselné hodnoty, požadavky nebo řešení RAMS pro konkrétní typy drážních zařízení.

Z hlediska technického řešení systému automatického vedení vlaku a jeho centrální řídící a diagnostické jednotky, modulu UniAVV, je vhodné jej posuzovat jako elektronický systém související s bezpečností. Norma ČSN EN 61508 Funkční bezpečnost elektrických /elektronických/programovatelných elektronických systémů souvisejících s bezpečností specifikuje požadavky pro všechny fáze životního cyklu hardware i software uvedených systémů. Pro jednotlivé úrovně integrity bezpečnosti (SIL) tato norma definuje konkrétní parametry bezporuchovosti hardware, které jsou požadovány pro dosažení požadované bezpečnosti systému.

Pro provádění analýzy spolehlivosti elektrotechnických systémů existuje řada kvalitativních a kvantitativních metod a nástrojů, jejichž postup je specifikován normami. Patří k nim:

- ČSN IEC 50(191) Mezinárodní elektrotechnický slovník – Kapitola 191: Spolehlivost a jakost služeb;
- ČSN IEC 812 Metody analýzy spolehlivosti systémů. Postup analýzy způsobů a důsledků poruch (FMEA);
- ČSN IEC 1025 Analýza stromů poruchových stavů (FTA);
- ČSN IEC 1078 Metody analýzy spolehlivosti. Metoda blokového diagramu bezporuchovosti;
- ČSN IEC 61703 Matematické výrazy pro termíny bezporuchovost, pohotovost, udržovatelnost a zajištěnost údržby;
- ČSN IEC 605 Zkoušky bezporuchovosti zařízení;
- MIL-HDBK-217F Reliability Prediction of Electronic Equipment (predikce bezporuchovosti elektronických zařízení); apod.

Pro prokázání dosažené úrovně spolehlivosti technických systémů je nezbytné předložení technické dokumentace dokládající postupy kvalitativního a kvantitativního hodnocení sledovaných ukazatelů a metody a výsledky jejich ověření. Tuto dokumentaci může pro výrobce technických systémů připravit řada specializovaných poradenských společností, nebo se na její realizaci může podílet některé z vysokoškolských pracovišť zabývající se problematikou spolehlivosti.

V České republice se problematice vzdělávání a vědeckovýzkumné činnosti v oblasti spolehlivosti věnují pracoviště následujících univerzit:

- Česká zemědělská univerzita v Praze, Technická fakulta – Katedra jakosti a spolehlivosti strojů;
- Univerzita obrany, Fakulta vojenských technologií – Katedra bojových a speciálních vozidel;
- Univerzita Pardubice, Dopravní fakulta Jana Pernera – Katedra dopravních prostředků a diagnostiky, Oddělení jakosti, spolehlivosti a diagnostiky;
- VŠB – Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky – Katedra aplikované matematiky;
- VŠB – Technická univerzita Ostrava, Fakulta strojní, Institut dopravy – Ústav dopravní techniky;
- Technická univerzita v Liberci, Fakulta mechatroniky a informatiky – Ústav řízení systémů a spolehlivosti.

V dalších zemích Evropské unie se problematikou spolehlivosti a bezpečnosti zabývají mimo jiné na pracovištích následujících univerzit:

- Faculté Polytechnique de Mons, Belgie – Risks Research Center;
- Bergische Universität Wuppertal, Německo – Section Safety Theory and Traffic Engineering;
- Technische Universität München, Německo – Institute for Safety and Reliability;
- City University London, School of Engineering and Mathematical Sciences, Velká Británie – Centre for Risk Management, Reliability, and Maintenance atd.

V oblasti spolehlivosti, bezpečnosti a hodnocení rizika technických systémů existuje velké množství tuzemských a zahraničních publikací a také velký počet odborných časopisů a specializovaných serverů, které poskytují řadu informací o teoretických metodách a přístupech i praktických řešeních problematiky. Mimo jiné k nim patří:

- časopis IEEE Transactions on Reliability (otázky bezporuchovosti, udržovatelnosti, pohotovosti, jakosti a bezpečnosti systémů kosmického průmyslu, komunikace, počítačů, průmyslové elektroniky, laserů, jaderné energetiky a dopravních systémů);
- časopis Microelectronics Reliability (časopis se věnuje oblasti bezporuchovosti mikroelektronických prvků, obvodů a systémů);

- časopis Reliability Engineering & System Safety (aplikace metod zlepšování bezpečnosti a spolehlivosti komplexních systémů, např. zařízení jaderné energetiky);
- server RIAC – Reliability Information Analysis Center (účelové zařízení Ministerstva obrany USA poskytuje všestrannou podporu v oblasti zabezpečování spolehlivosti, tj. publikace, software, vzdělávací aktivity, databáze informací o bezporuchovosti mechanických a elektronických prvků apod.);
- server Weibull.com (web provozovaný společností ReliaSoft, která je výrobcem software pro kvalitativní a kvantitativní analýzu spolehlivosti, pro jednotlivé programy jsou k dispozici bezplatné demo verze, příručky použití a elektronické učební texty).

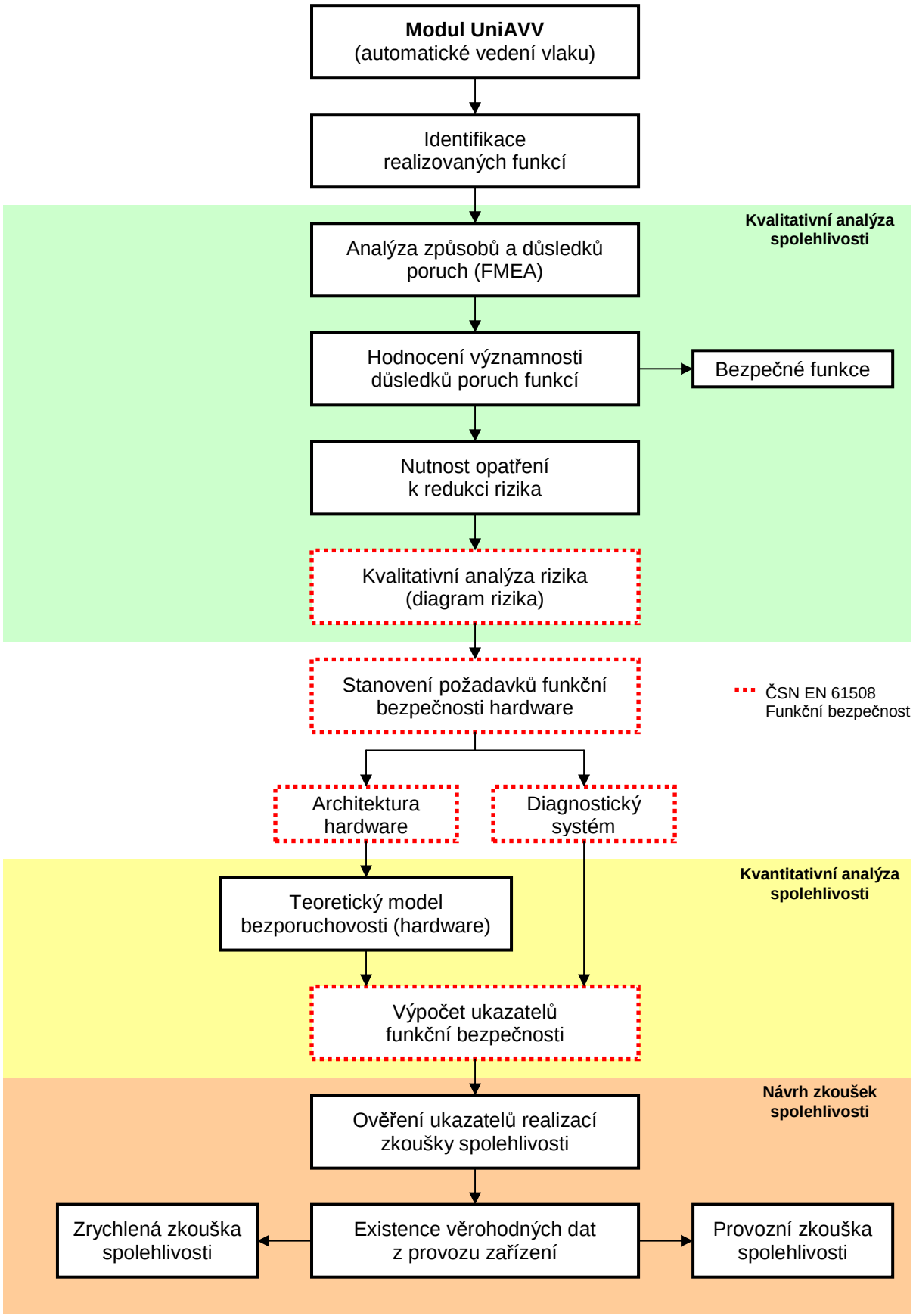
Pro hodnocení a ověření spolehlivosti elektrotechnických systémů tedy existuje celá řada zdrojů, informací a nástrojů. Ty mohou výrobcům těchto zařízení usnadnit prokazování skutečné úrovně posuzovaných parametrů bezporuchovosti, bezpečnosti apod.

1.2 Cíle disertační práce

Náplní této disertační práce je provedení analýzy spolehlivosti modulu UniAVV, který je centrální řídící a diagnostickou jednotkou systému automatického vedení vlaku (AVV). S využitím existujících metod je provedena analýza možných poruch systému a výpočtem stanoveny základní charakteristiky spolehlivosti, hodnotící jeho bezporuchovost a bezpečnost. Pro systém je v práci navržen program zkoušek spolehlivosti pro ověření skutečné úrovně spolehlivosti modulu UniAVV (schematicky je náplň práce zobrazena na obr. č. 1.1).

Cíle disertační práce „Stanovení spolehlivostních charakteristik nové generace modulu automatického vedení vlaku (AVV)“ jsou tedy definovány následovně:

- Provést kvalitativní analýzu spolehlivosti systému automatického vedení vlaku se zaměřením na analýzu možných způsobů a důsledků poruch.
- Provést výpočet charakteristik spolehlivosti systému automatického vedení vlaku vycházející z parametrů spolehlivosti jeho tvořících prvků.
- Stanovit podmínky a navrhnout postup provádění a vyhodnocení zkoušek spolehlivosti v rámci experimentálního ověření parametrů spolehlivosti systému automatického vedení vlaku.
- Navrhnout opatření vedoucí ke zvýšení úrovně spolehlivosti systému automatického vedení vlaku, pokud budou na základě výsledků předchozích kroků žádoucí.



Obr. č. 1.1: Schéma analýzy spolehlivosti modulu UniAVV

2 FUNKCE, STRUKTURA A VAZBY SYSTÉMU AVV

Se zvyšující se rychlostí jízdy vlaků, která souvisí s modernizací tratí stávajících a stavbou nových vysokorychlostních tratí, roste také četnost vjemů, které působí na strojvedoucího řídícího hnací vozidlo. To s sebou přináší nutnost rychlejších reakcí, vyšší psychickou zátěž a tudíž negativní vliv lidského činitele na bezpečnost železničního provozu. Tyto skutečnosti vedly s rozvojem automatizace k vývoji systému automatického řízení vlaku.

Systémy automatizace při řízení kolejových vozidel se v České republice využívají více než 40 let, kdy byl poprvé zaveden regulátor rychlosti u motorového vozu. Vývoj systémů automatizace pokračoval zavedením systémů cílového brzdění a následně regulátoru jízdní doby. V současné době jsou využívány digitální regulátory, které umožňují plně realizovat funkci automatického vedení vlaku.

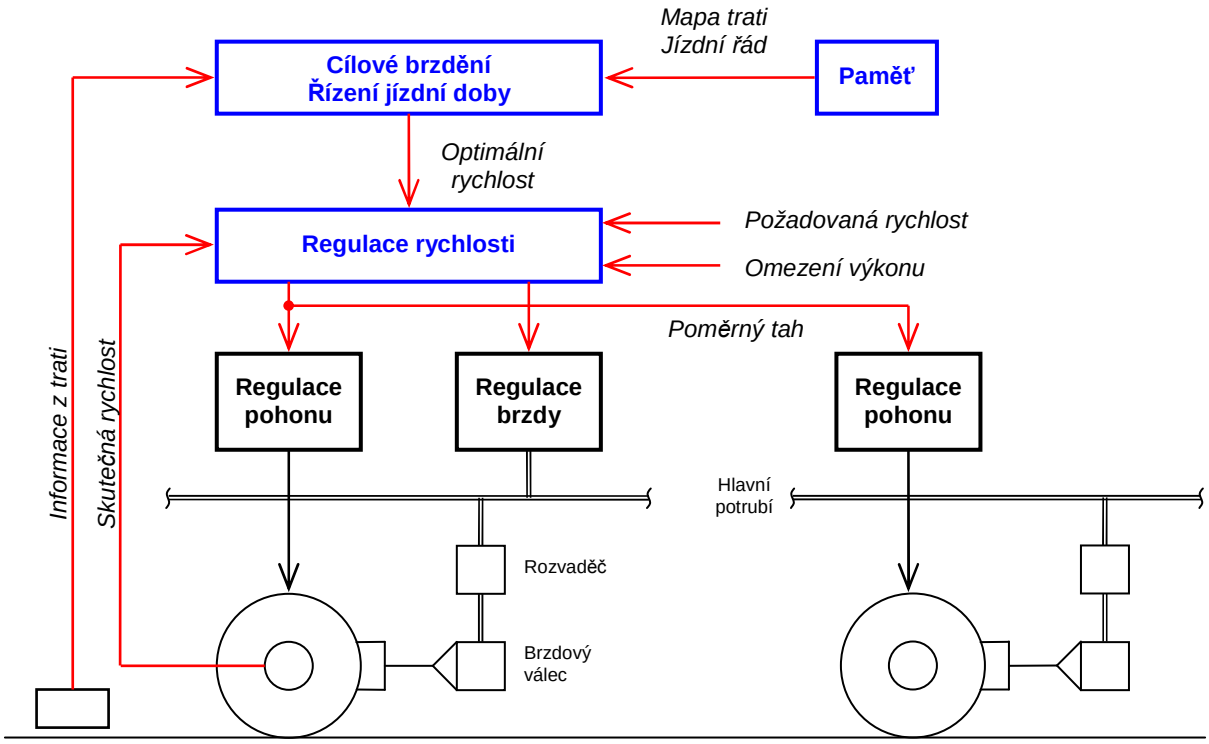
K hlavním přednostem stále většího využívání systémů automatického řízení kolejových vozidel patří mimo zvýšení bezpečnosti provozu také zmenšení pracovního zatížení strojvedoucího, úspory trakční energie a tedy menší zatížení životního prostředí, efektivnější dodržování jízdního řádu apod.

2.1 Základní principy a funkce

Systém používaný v České republice pro automatické řízení vlaku je označován jako systém automatického vedení vlaku (AVV). Svými funkcemi odpovídá systémům, které jsou v zahraniční označovány jako ATO (Automatic Train Operation).

Zařízení automatického vedení vlaku do značné míry nahrazuje funkce strojvedoucího řídícího kolejové vozidlo. Činnost systému AVV avšak nepřejímá zodpovědnost strojvedoucího nad jízdou vlaku a strojvedoucí má možnost do činnosti automatického řízení kdykoliv zasáhnout a řídit vozidlo v manuálním režimu. K základním funkcím systému automatického vedení vlaku tedy patří navádění na požadovanou rychlost a její udržování a cílové brzdění k místům se sníženou rychlostí a k místům zastavení. Další funkcí, kterou systém vykonává a která z hlediska řízení vlaku strojvedoucím může představovat obtížnou činnost a vyžaduje značné praktické zkušenosti, je optimalizace jízdy vlaku, zahrnující jízdu vlaku podle jízdního řádu při nejnižší možné spotřebě energie.

Základní funkce systému AVV v blokovém schématu společně s vazbami na hlavní celky vozidla určené pro řízení jeho jízdy jsou uvedeny na obr. č. 2.1 [3].



Obr. č. 2.1: Blokové schéma funkcí systému AVV

Automatická regulace rychlosti

Funkce automatické regulace rychlosti představuje aperiodické navádění na požadovanou rychlost (bez překmitů a podkmitů), tedy tak, aby při dosažení požadované rychlosti bylo zrychlení vlaku právě nulové.

Automatická regulace rychlosti se provádí řízením pohonu hnacího vozidla (tažná síla, elektrodynamická brzda) a pneumatické brzdy vlaku prostřednictvím veličiny označované jako poměrný tah. Poměrný tah může nabývat hodnot od +100 % (maximální výkon vozidla omezený trakční charakteristikou) až do -100 % (maximální brzdná síla), přičemž pro brzdění se přednostně využívá elektrodynamická brzda, jejíž nedostatečný účinek může být doplněn pneumatickou brzdou (doplňková brzda) [10].

Možnost realizace funkce automatické regulace rychlosti vyžaduje nepřetržité informace o skutečné rychlosti vozidla, resp. o jeho okamžitém zrychlení (daném jako

derivace měřené rychlosti). Sledování rychlosti vozidla je provedeno prostřednictvím snímačů otáček dvojkolí v provedení, které zajišťuje dostatečnou spolehlivost a dokáže zabránit ztrátě signálu při skluzu (smyku) dvojkolí.

Cílové brzdění

Základní funkcí cílového brzdění, která je vykonávána systémem AVV, je navedení vlaku na cílovou rychlost právě v definovaném místě na trati. Cílové brzdění je realizováno k návěstidlům (s návěstí pro omezení rychlosti nebo zastavení), k místům zastavení (nástupiště stanic a zastávek) a k místům s trvalým nebo dočasným omezením traťové rychlosti [10].

Funkce cílového brzdění představuje řešení složité úlohy. Do výpočtu vstupují kromě signálu o okamžité rychlosti vozidla také informace o aktuální poloze vozidla na trati, poloze stanovených cílů, dovolené rychlosti a sklonových poměrech trati. Při realizaci úlohy cílového brzdění je nutné stanovit vzdálenost od cíle, ve které začne realizace cílového brzdění.

Realizace funkce cílového brzdění vlaku je možná pouze v případě, že je trať vybavená informačními body, které jednoznačně identifikují okamžitou polohu vozidla. Na základě určené polohy systém AVV načítá z palubní mapy trati všechny potřené informace o trati (sklonový profil, rychlostní profil, polohy návěstidel, místa zastavení na zastávkách atd.).

Přenos informací z traťového zabezpečovacího systému pro systém AVV je zajištěn prostřednictvím liniového vlakového zabezpečovače, resp. systému ETCS. Přenos informací z tratě je popsán v kapitole 2.3.

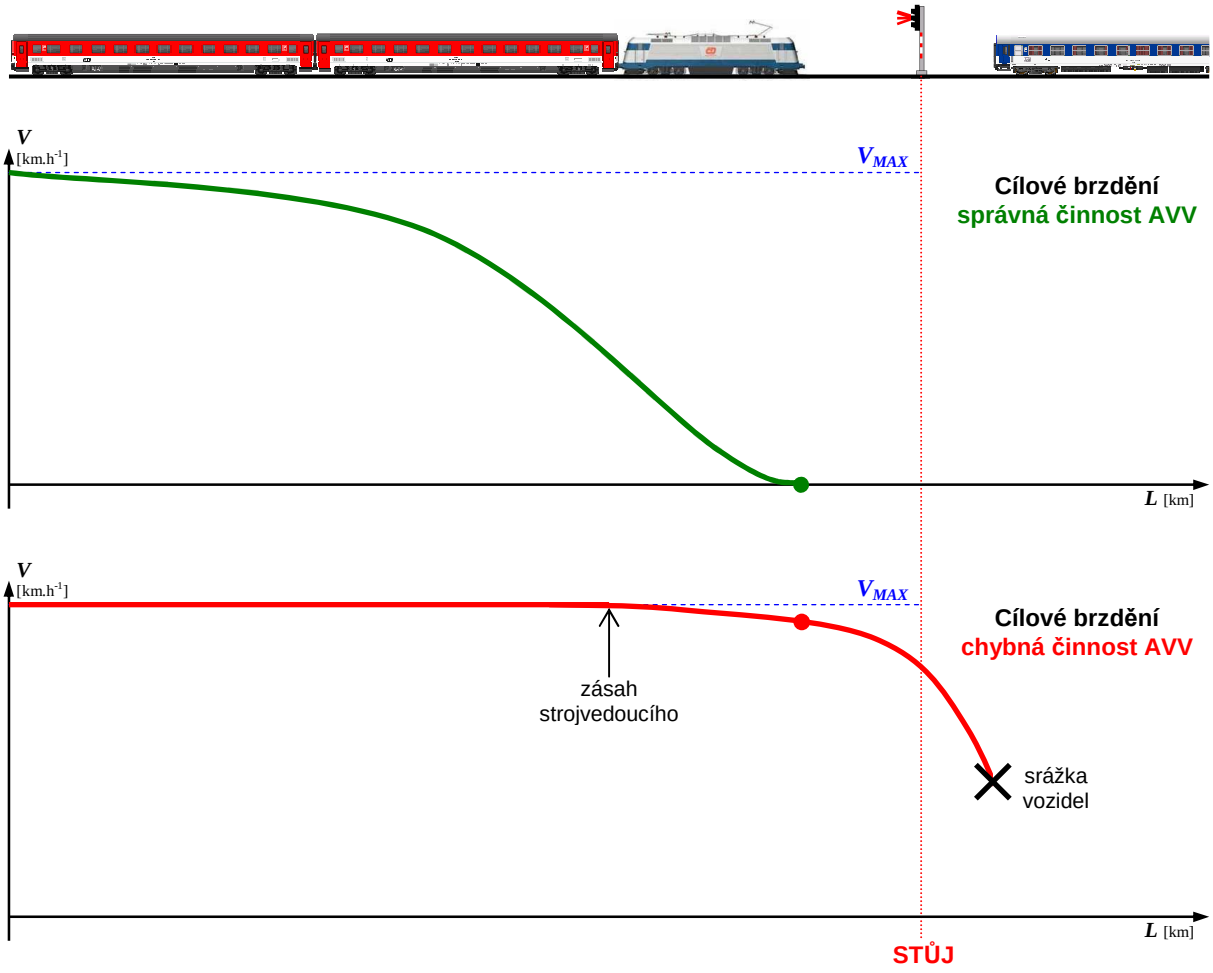
Optimalizace jízdy vlaku

Optimalizátor jízdy vlaku řeší úlohu regulace jízdní doby a energetickou optimalizaci jízdy vlaku. Cílem je řídit jízdu vlaku tak, aby byl dodržen jízdní řád a zároveň spotřeba energie byla co nejnižší.

Tato jízdní strategie je realizována zavedením výběhu hnacího vozidla ve vhodný okamžik. Při jízdě výběhem, kdy se vlak pohybuje pouze setrvačností, je spotřeba trakční energie nulová, ale současně dochází k nárůstu jízdní doby. Výrazného snížení spotřeby se dosáhne rozjezdem s maximálním zrychlením (s respektováním adhezních podmínek),

zavedením výběhu tak, aby byla dodržena stanovená jízdní doba, a brzděním s maximálním možným zpomalením [3].

Funkce optimalizace jízdy vlaku je součástí funkce cílového brzdění systému AVV. Pro její realizaci navíc systém využívá palubního jízdního řádu, v němž jsou obsaženy informace o jízdě vlaku (zastávky a stanice, ve kterých vlak zastavuje, a doby příjezdů a odjezdů).



Obr. č. 2.2: Ilustrace funkcí AVV – vznik nebezpečné události

Z uvedených charakteristik funkcí systému automatického vedení vlaku je zřejmé, že jejich činnost je spojena s bezpečností provozu železniční dopravy. Porucha funkce systému AVV nebo jeho nesprávná činnost vede ke vzniku rizika spojeného s možným ohrožením lidského zdraví a životů, případně životního prostředí. K těmto nebezpečným událostem může dojít i přesto, že za řízení vozidla je i při činnosti systému AVV zodpovědný strojvedoucí,

neboť je nutné zohlednit vznik krajně nepravděpodobné kombinace nebezpečných vlivů, případně vliv selhání lidského činitele.

Nebezpečnou událost může vyvolat porucha funkce automatické regulace rychlosti, kdy se vozidlo (vlak) pohybuje rychlostí vyšší, než je nejvyšší dovolená rychlost. V krajním případě může tato situace vést až k vykolejení vozidel.

Vznik nebezpečných událostí je spojen také s poruchou funkce cílového brzdění systému AVV. Nesprávná identifikace vozidla na trati nebo chybný přenos informací z traťového zabezpečovacího zařízení apod. může způsobit, že cílové brzdění vlaku není realizováno adekvátně pro aktuální situaci. To může vést k krajním případě k vykolejení vozidel, nebo srážce vlaků. Ilustrace ohrožení bezpečnosti vlivem nesprávné činnosti systému AVV při cílovém brzdění k návěstidlu s návěstí „Stůj“ je uvedena na obr. č. 2.2 výše.

2.2 Mobilní část systému AVV

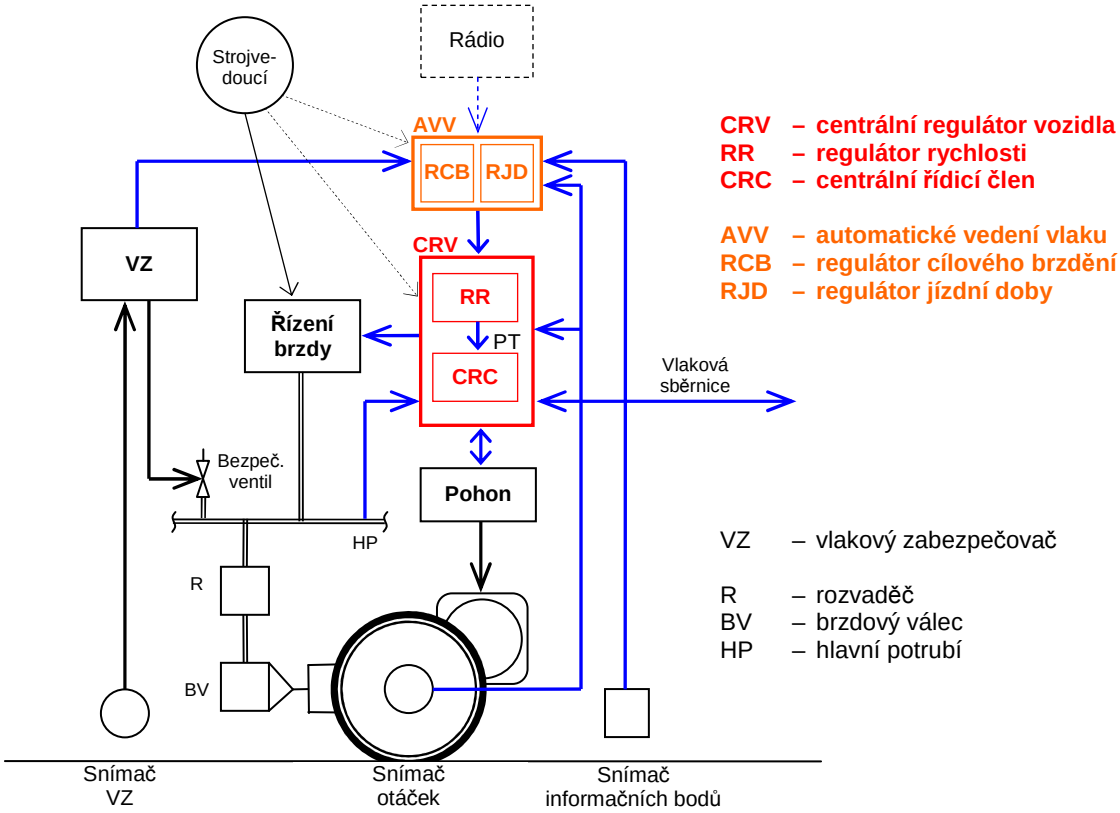
Realizaci funkcí systému automatického vedení vlaku vykonává palubní část systému, která je začleněná do řídícího systému hnacího vozidla. Tvoří ji dva základní funkční bloky:

- CRV – centrální regulátor vozidla,
- AVV – blok automatického vedení vlaku.

Centrální regulátor vozidla obsahuje regulátor rychlosti (RR) a člen CRC (centrální řídicí člen). Tento člen zajišťuje řízení pohonu a brzdových systémů hnacího vozidla. Umožňuje také násobné řízení hnacích vozidel zařazených ve vlaku (pokud jsou vybaveny systémem AVV) prostřednictvím řídicí vlakové sběrnice [10].

Blok automatického vedení vlaku vykonává funkce cílového brzdění a optimalizace jízdy vlaku. Při násobném řízení hnacích vozidel je tato funkce aktivní pouze na vedoucím vozidle vlaku. Řízení vozidla (vozidel) v tomto režimu je možné pouze na tratích vybavených traťovou částí systému AVV (informační body, balízy).

Níže uvedený obr. č. 2.3 zobrazuje základní blokové schéma palubní části systému AVV se začleněním do systému řízení hnacího vozidla.



Obr. č. 2.3: Blokové schéma systému AVV

2.2.1 Modul automatického vedení vlaku UniAVV

U moderní, v současné době vyráběné, třísystémové lokomotivy Škoda 109 E (řada 380 ČD, popis viz příloha č. 1) je mobilní část systému AVV tvořena modulem UniAVV, jehož vývoj a výrobu zajišťuje společnost MSV elektronika s.r.o.

Modul automatického vedení vlaku UniAVV je součástí nadřazeného procesorového řídícího systému vozidla, který ovládá a řídí trakční a brzdové systémy a pomocné pohony hnacího vozidla a umožňuje násobné řízení hnacích vozidel (aktivních i neaktivních) prostřednictvím pokynů zadávaných hlavní jízdní pákou a dalšími ovládacími prvky na pultu strojvedoucího, nebo prostřednictvím pokynů z modulu UniAVV. S ostatními řídicími subsystémy vozidla komunikuje modul UniAVV prostřednictvím vozidlového počítače (VTCU) [14].

Konstrukce modulu UniAVV představuje samostatný zásuvný modul, který je možné instalovat přímo do vozidlového počítače nebo do samostatné skříně. Modul je složen ze tří desek s plošnými spoji, přičemž každá deska je osazena procesorem, který řeší své specifické

úkoly. Vzájemné propojení desek je realizováno interní linkou CAN. Komunikace s vozidlovým počítačem VTCU je zajištěna přes dvě dvoubránové paměti RAM, ke kterým VTCU přistupuje prostřednictvím externí paralelní sběrnice. Pro přenos povelů pro modul UniAVV od strojvedoucího je využívána klávesnice pro ARR a AVV, k zobrazení informací slouží provozní a diagnostický displej vozidla. Tyto prvky jsou umístěny na obou pultech strojvedoucího [14].

Vstupním signálem, který modul UniAVV využívá pro funkci automatické regulace rychlosti, jsou otáčky dvojkolí, které jsou snímány na všech dvojkolích, a na jejich základě se určuje rychlost jízdy vozidla.

K dalším vstupním signálům modulu UniAVV, které jsou nutné pro režimy cílového brzdění a optimalizace jízdy vlaku, patří signál ze snímače magnetických informačních bodů a signál z vlakového zabezpečovače.

Ze snímače magnetických informačních bodů jsou do modulu UniAVV přenášeny signály o rozmístění magnetů v MIB (pravý sever, pravý jih, levý sever a levý jih), přičemž modul je vybaven diagnostickým systémem snímačů MIB. Snímač MIB je rovněž uzpůsoben pro čtení signálů z traťové části ETCS (eurobalízy).

Z vlakového zabezpečovače typu LZB 80E jsou přenášeny signály zelené světlo, žluté světlo, žluté mezikruží a červené světlo. Součástí „národního“ zabezpečovače je specifický přenosový modul STM (Specific Transmission Module) [12], který je využíván pro komunikaci se systémem ERTMS/ETCS. Po rozšíření systému ERTMS/ETCS bude modul UniAVV přebírat informace pouze od tohoto zabezpečovacího systému.

Modul UniAVV je tvořen třemi deskami (ATO, TBA, IO), přičemž procesor každé z nich řeší své specifické úkoly [14], viz níže.

Software desky ATO řeší základní úlohu nadřazeného řízení vozidla, kterou je možné rozčlenit následovně:

- modul CRV řeší úlohy vlastního řízení vozidla, přijímá signály z desky IO nebo vozidlového počítače VTCU, vyhodnocuje rychlost otáčení dvojkolí a provádí diagnostiku jejich snímačů, ovládá výstupy prostřednictvím desky IO nebo VTCU, provádí automatickou regulaci rychlosti (ARR), zajišťuje součinnost brzd a protiskluzovou/protismykovou ochranu, vyhodnocuje signály ze snímačů MIB a provádí jejich diagnostiku, zabezpečuje komunikaci systému s okolím,

- modul RCB řeší úlohu detekce polohy vozidla na trati, provádí analýzu situace a určuje požadovanou rychlost pro modul regulace rychlosti ARR,
- modul OJV zajišťuje sestavení statického rychlostního profilu, provádí odhad nejkratší jízdní doby a zajišťuje optimální jízdní strategii,
- modul USR (uživatelské sériové rozhraní) je určen pro údržbu map tratí, obsahuje také záznamový podsystém vybraných veličin,
- modul AVV je spouštěcí modul, zajišťující vytvoření prostředí pro běh aplikace.

Software desky TBA řeší především úlohu přenosu dat prostřednictvím řídící a diagnostické linky vlakové komunikační sběrnice NVL ČD. Software desky IO zajišťuje čtení vstupních signálů, včetně příslušné ochrany proti rušení, a nastavování výstupů a jejich diagnostiku.

Řídicí systém lokomotivy 109 E je řešen jako redundantní, proto i modul UniAVV je ve vozidle ve zdvojeném provedení. Při běžném provozu jsou v činnosti oba moduly UniAVV, přičemž požadované funkce vykonává pouze jeden z nich. V případě poruchy jednoho z modulů je jeho činnost nahrazena záložním zařízením.

2.3 Traťová část systému AVV

Pro realizaci funkcí cílového brzdění a optimalizace jízdy vlaku, zajišťovaných systémem automatického vedení vlaku, je nutné mít k dispozici informace o tom, v jakém místě traťového úseku se vozidlo nachází a jaký je stav zabezpečení vlakové cesty v traťovém úseku před pohybujícím se vlakem.

2.3.1 Informace o poloze vozidla

Pro určení polohy vozidla na trati je využívána traťová část systému AVV, která je v současné době tvořena tzv. magnetickými informačními body (MIB). Jejich rozmístění je závislé na typu trati (mezistaniční úseky, zhlaví železničních stanic, místa odjezdových návěstidel apod.).

Magnetický informační bod je umístěn podélně v ose koleje a je tvořen dvěma dřevěnými, resp. plastovými trámy, v jejichž dvanácti otvorech je rozmístěno osm permanentních magnetů. Rozmístění a polarita magnetů (sever, jih) udávají jedinečnou informaci o poloze vozidla a směru jeho projíždění přes informační bod [11].

V mezistaničních úsecích trati se informační body používají především k aktualizaci (upřesnění) polohy pohybujícího se vozidla. Přečtení informačního bodu tak představuje potvrzení očekávané informace o poloze vozidla, která je specifikována polohou informačního bodu uvedenou v palubní mapě trati.

Na zhlavích železničních stanic, kde dochází ke kolejovému rozvětvení, musí být informační bod umístěn v každé koleji, která je určena pro jízdu vozidel v režimu AVV. Přečtení informačního bodu představuje informaci o skutečném pokračování vlakové cesty, přičemž do tohoto okamžiku systém AVV předpokládá jízdu po hlavní koleji.

Je zřejmé, že správný a spolehlivý přenos informace z informačního bodu o poloze vozidla je důležitý z hlediska bezpečnosti provozu železniční dopravy. Nebezpečná situace představuje chybné přečtení informace z MIB a její akceptování, čímž dojde k nesprávnému určení polohy vozidla.

U používaných informačních bodů je bezpečnost přenosu zajištěna redundancí přenášených zpráv, kdy platné zprávy tvoří pouze část z přenositelných informací a ty se od sebe co nejvíce liší. U binárních zpráv je toto vyjádřeno tzv. Hammingovým odstupem, tedy počtem bitů, v nichž se platné zprávy navzájem liší [11]. S rostoucí hodnotou Hammingova odstupu tak klesá pravděpodobnost současného chybného přečtení daného počtu bitů, čímž se snižuje možnost chybného určení polohy vozidla.

Informační body umístěné v mezistaničních úsecích bez kolejového rozvětvení mají Hammingův odstup $H = 2$. Pro snížení pravděpodobnosti chybného přečtení informace MIB a dosažení vyšší úrovně Hammingova odstupu, např. požadovaných $H = 8$, dochází k tvorbě tzv. řetězových kódů, tj. fiktivní slučování více za sebou položených MIB, společně s využitím palubní části systému AVV (mapy tratě) [11]. Porovnáním informací o MIB uložených v palubní mapě trati s informacemi přenášenými z trati lze okamžitě detekovat chybné přečtení MIB, neboť na širé trati lze očekávat vždy pouze jeden konkrétní MIB.

U informačních bodů umístěných na zhlavích, kdy je možná jízda vlaku ve více směrech, musí být požadovaná hodnota Hammingova odstupu $H = 8$ zajištěna tím, že informační zprávy jednotlivých MIB se liší o uvedený počet 8 bitů. Pak pravděpodobnost, že dojde k nesprávnému přečtení 8 bitů současně, a tím k nesprávnému určení koleje zhlaví, na které se vlak nachází, je velmi nízká.

2.3.2 Informace ze zabezpečovacího systému

Pro možnost realizace funkce cílového brzdění, která zahrnuje také zastavení vlaku před návěstidlem zakazujícím jízdu nebo snížení rychlosti na úrovni návěstidla omezujícího rychlost vlaku, je nutné, aby systém AVV získával informace z traťového zabezpečovacího zařízení. Tyto informace jsou přenášeny z traťové části vlakového zabezpečovače do mobilní části umístěné ve vozidle, odkud je přejímá systém AVV.

V České republice je na železničních tratích a vozidlech instalovaný systém liniového vlakového zabezpečovače (LVZ) s označením LS90. LVZ je určen pro kontrolu bdělosti strojvedoucího a přenos návěstních znaků na stanoviště strojvedoucího prostřednictvím návěstního opakovače. Systém přenáší návěsti stůj, výstraha, volno a návěst, která přikazuje jízdu sníženou rychlostí.

Systém AVV přejímá od LVZ indukčně oddělený signál, aby se zabránilo zpětnému ovlivnění činnosti LVZ při poruše systému AVV. Systém vlakového zabezpečovače je systému AVV nadřazen a systém AVV do jeho činnosti nijak nezasahuje. LVZ předává systému AVV na kódovaných tratích signál návěstního znaku návěstidla, ke kterému se vlak přibližuje, přičemž u vícepovolujících znaků je provedeno převedení na nejzávažnější návěst, pokud není strojvedoucím tento znak upřesněn (např. namísto návěsti Výstraha může strojvedoucí zadat návěst Očekávej 80). Systém AVV na kódovaných tratích realizuje cílové brzdění tak, aby nemuselo dojít k zásahu LVZ [10].

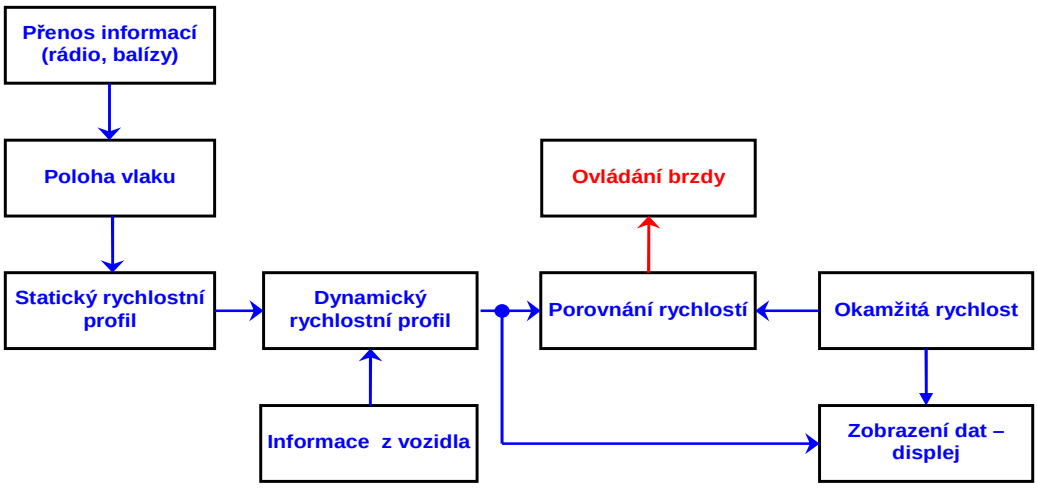
V současné době je u evropských železnic využívána celá řada národních vlakových zabezpečovačů, které mají různé funkce, odlišnou úroveň zabezpečení a jsou vzájemně nekompatibilní, což snižuje interoperabilitu a tedy větší využitelnost vozidel v celoevropském měřítku. Tyto nevýhody jsou v současné době odstraňovány postupným zaváděním jednotného evropského zabezpečovacího systému ERTMS/ETCS.

Cílem Evropského rámcového programu ERTMS (European Rail Traffic Management System) je vytvořit standardizovaný evropský systém železnic, který povede ke zlepšení bezpečnosti, spolehlivosti, výkonnosti a interoperability železniční dopravy. Program ERTMS se skládá ze dvou základních částí:

- zabezpečovacího systému ETCS (European Train Control System), který přenáší na stanoviště strojvedoucího informace o povolené rychlosti vlaku a neustále kontroluje její dodržování, při jejím překročení aktivuje provozní, resp. rychločinné brzdění;

- zařízení pro komunikaci mezi jednotlivými prvky drážní sítě na bázi systému GSM-R, určeného pro výměnu hlasových a datových informací [12].

Systém ERTMS/ETCS je tvořen částí traťovou a částí mobilní, umístěnou ve vozidle. Traťová část systému generuje pro daný vlak tzv. oprávnění k jízdě, včetně statického jízdního profilu. Tyto informace jsou přenášeny pomocí rádia sítí GSM-R na vozidlo. Dalšími komunikačními prvky traťové části systému jsou eurobalízy (pevné, přepínatelné), určené pro identifikaci polohy vlaku na trati, a smyčky pro liniový přenos informací na vozidlo. Mobilní část systému ETCS transformuje statický rychlostní profil na základě informací z vozidla na dynamický rychlostní profil, který představuje průběh dovolené rychlosti vlaku před místy s omezením rychlosti (brzdové křivky). Principiální schéma systému ERTMS/ETCS je zobrazeno na obr. č. 2.4 [12].



Obr. č. 2.4: Principiální schéma systému ERTMS/ETCS

Spolupráce zabezpečovacího systému ETCS se systémem AVV v režimu cílového brzdění je možná s využitím statického rychlostního profilu, který systém AVV přebírá od systému ETCS. Na základě těchto informací systém AVV realizuje cílové brzdění tak, aby nedošlo k překročení dovolené rychlosti stanovené systémem ETCS, dané dynamickým rychlostním profilem, a tudíž k aktivaci brzdového systému vlaku.

Na tratích vybavených eurobalízami lze u vozidel vybavených mobilní částí ETCS přejímat přes definované rozhraní informace o poloze vozidla také pro činnost systému AVV. V tomto případě je funkce cílového brzdění realizovatelná bez nutnosti použití v současné době využívaných magnetických informačních bodů [10].

3 ANALÝZA SPOLEHLIVOSTI S VYUŽITÍM PRINCIPŮ FUNKČNÍ BEZPEČNOSTI

Bezpečnost technických zařízení je ovlivňována velkým množstvím faktorů. Významný činitel představuje spolehlivost, kdy porucha zařízení, ať systematická nebo náhodná, může mít kritický vliv na bezpečný provoz systému. Pro jednotné hodnocení bezpečnosti systémů je žádoucí existence standardů, které by zaručily konzistentní přístup ke kvalitativním i kvantitativním faktorům ovlivňujícím bezpečnost.

Principy hodnocení funkční bezpečnosti elektrických, elektronických a programovatelných elektronických systémů souvisejících s bezpečností, jsou stanoveny mezinárodní normou ČSN EN 61508. Tato norma stanovuje přístupy hodnocení bezpečnosti hardware a software ve všech fázích životního cyklu celkové bezpečnosti od stanovení koncepce a návrhu, přes vývoj a realizaci, provoz a údržbu, až po vyřazení z provozu. Hlavním cílem použití systémů souvisejících s bezpečností je snížení rizika vyplývajícího z činnosti zařízení prostřednictvím aplikace ochranných systémů založených na různých technických principech.

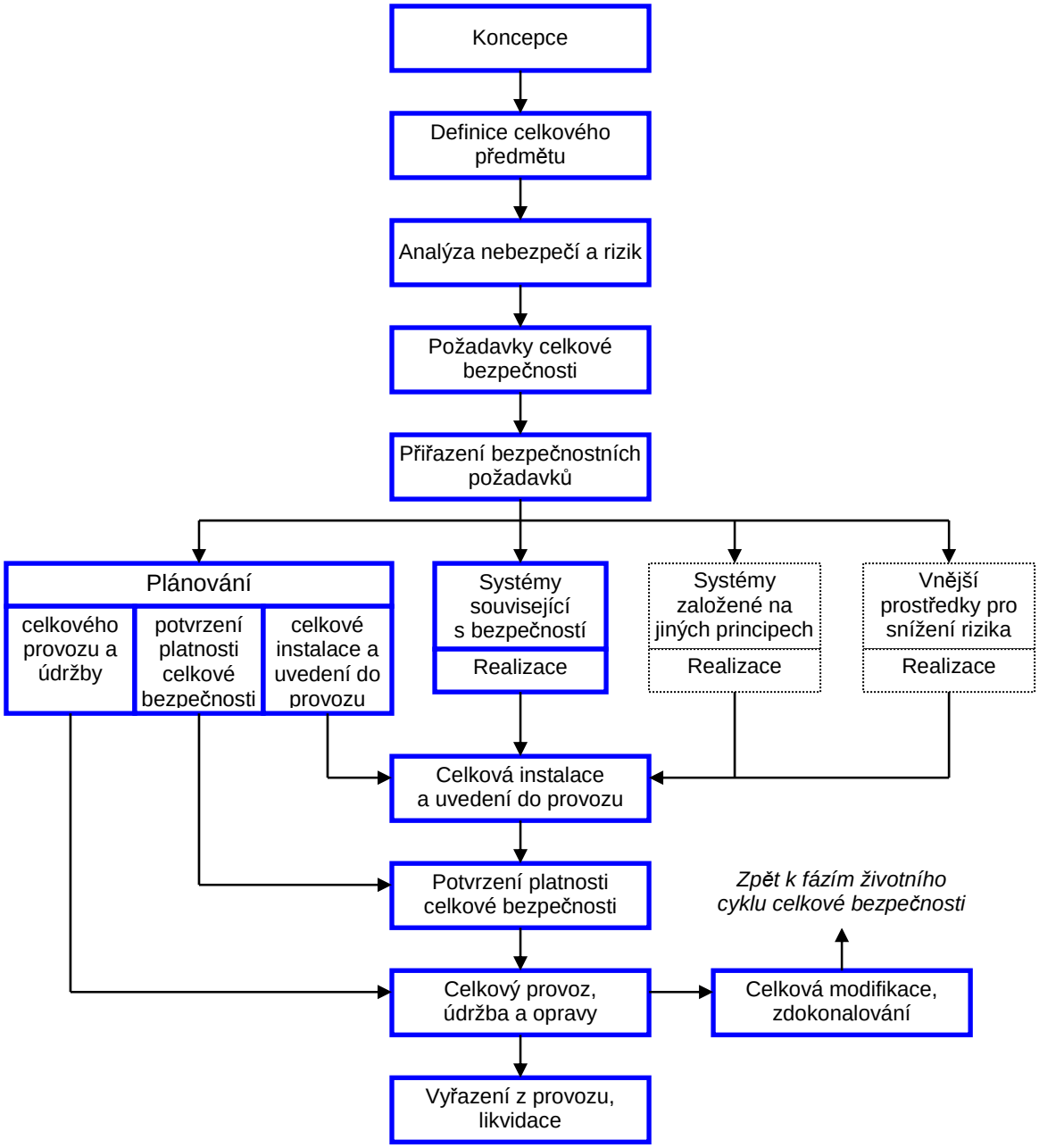
Požadovaná úroveň funkční bezpečnosti u výše uvedených systémů je zajišťována realizací bezpečnostních funkcí. Specifikace bezpečnostních požadavků na tyto funkce je provedena na základě analýzy rizika systému přiřazením cílové úrovně integrity bezpečnosti (SIL). Pro jednotlivé úrovně integrity bezpečnosti jsou specifikovány konkrétní číselné hodnoty pravděpodobnosti poruchy, které jsou požadovány pro zajištění stanovené úrovně bezpečnosti systému.

3.1 Základní principy

Norma ČSN EN 61508 je určena zejména pro systémy související s bezpečností, jestliže jsou založeny na principu elektrických, elektronických nebo programovatelných elektronických systémů (dále v textu označovány jako systémy E/E/PE). Její použití je vhodné zejména v případě, kdy porucha těchto systémů by mohla mít dopad na bezpečnost osob nebo okolního prostředí, případně by porucha mohla způsobit vážné ekonomické následky [15].

3.1.1 Životní cyklus celkové bezpečnosti

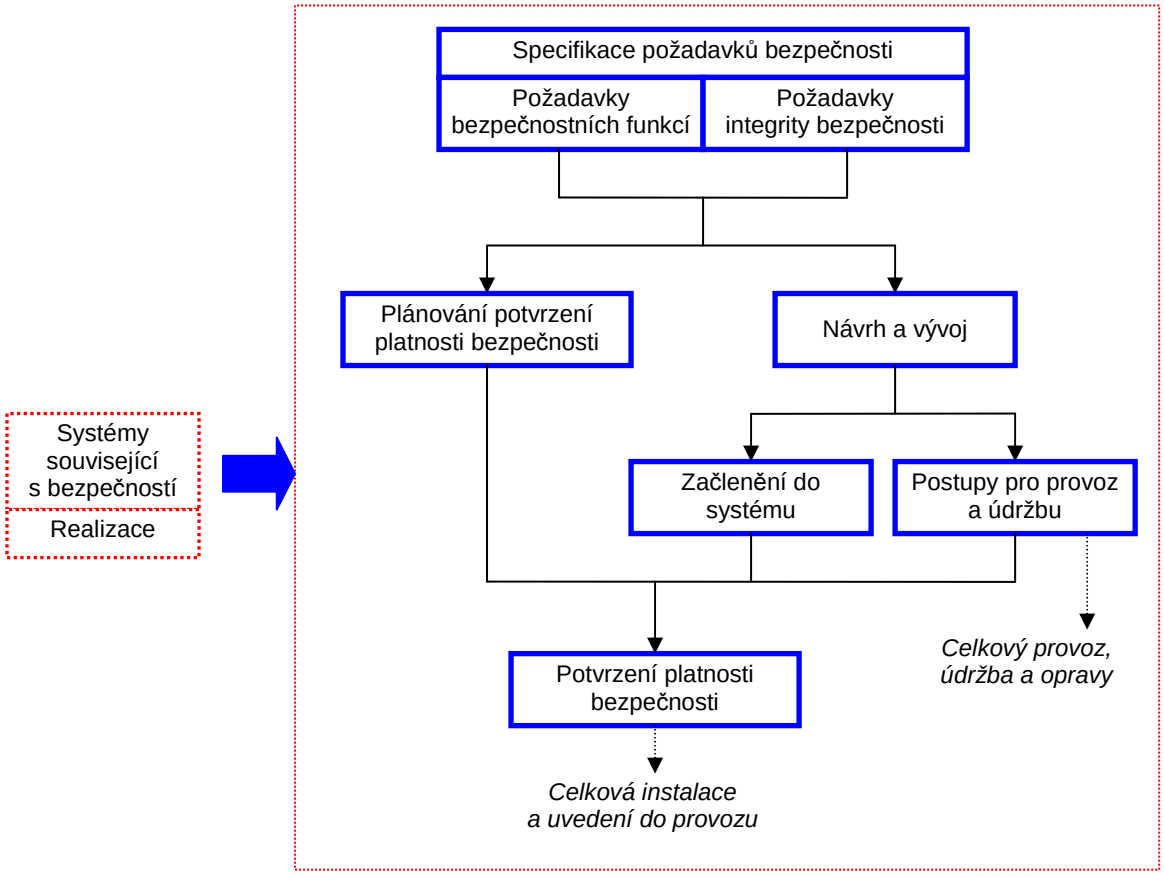
Technický rámec pro aplikaci funkční bezpečnosti u systémů souvisejících s bezpečností je zajištěn prostřednictvím životního cyklu celkové bezpečnosti, který je zobrazen na obr. č. 3.1. Provádění činností v jednotlivých fázích tohoto cyklu je zajišťováno prostřednictvím managementu funkční bezpečnosti, který je zaměřen zejména na strategii dosažení funkční bezpečnosti, odpovědnost osob a organizací za provádění a kontrolu aktivit, vedení dokumentace, analýzu vzniklých nebezpečných událostí, sledování provozu a údržby zařízení, organizaci prověrek funkční bezpečnosti apod.



Obr. č. 3.1: Životní cyklus celkové bezpečnosti

Přestože se norma ČSN EN 61508 zabývá především systémy souvisejícími s bezpečností založenými na principu elektrických, elektronických nebo programovatelných elektronických systémů (E/E/PE systémy), jsou v životním cyklu celkové bezpečnosti zahnuty také systémy související s bezpečností založené na jiných technických principech a vnější prostředky pro snížení rizika, jejichž součinnost vede k efektivnímu snížení rizika systému na přijatelnou úroveň.

Požadavky funkční bezpečnosti, vyplývající z jednotlivých fází životního cyklu celkové bezpečnosti pro E/E/PE systémy, jsou stanoveny zvlášť jak pro hardware, tak i pro software systémů souvisejících s bezpečností. Životní cyklus hardware E/E/PE systémů je uveden na obr. č. 3.2 [15]. Funkční bezpečnost software těchto systémů nebude dále detailněji zmiňována z důvodu zaměření sledované problematiky v této práci.



Obr. č. 3.2: Životní cyklus hardware E/E/PE systémů

Základní princip systémů souvisejících s bezpečností založených na principu E/E/PE systémů je založen na snížení rizika tzv. řízených zařízení (EUC) s vlastním systémem řízení.

Pokud není systém související s bezpečností oddělený a nezávislý na systému řízení EUC, pak i systém řízení EUC musí být řešen jako systém související s bezpečností. Požadavky na funkční bezpečnost vycházejí z důkladného poznání a analyzování řízeného zařízení (EUC).

Jednotlivé fáze životního cyklu celkové bezpečnosti mají definované cíle a požadavky, které mají být aplikovány pro E/E/PE systémy za účelem zajištění jejich funkční bezpečnosti. Pro každou fázi cyklu je pak stanoven ověřovací plán, pomocí kterého se prokáže (posouzením, analýzou, zkouškami), že výstupy fáze splňují všechny stanovené cíle a požadavky.

3.1.2 Úroveň integrity bezpečnosti

Základní ukazatel funkční bezpečnosti systémů E/E/PE představuje úroveň integrity bezpečnosti (Safety Integrity Level, SIL). Pro tento ukazatel jsou definovány čtyři hodnoty od SIL 1 po SIL 4, přičemž vyšší hodnota představuje vyšší úroveň funkční bezpečnosti systému.

Přiřazení úrovně integrity bezpečnosti u E/E/PE systémů, případně systémů založených na jiných technických principech, se provádí tak, aby se u daného systému souvisejícího s bezpečností dosáhlo snížení rizika na přijatelnou úroveň.

Ukazatel SIL charakterizuje integritu bezpečnosti systémů E/E/PE, která vyjadřuje pravděpodobnost, že systém související s bezpečností plní požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu [17]. Integrita bezpečnosti zahrnuje jak integritu bezpečnosti hardware (týkající se náhodných nebezpečných poruch systému), tak i systematickou integritu bezpečnosti (související se systematickými poruchami systému).

Parametr úrovně integrity bezpečnosti je označován jako cílová míra poruch a je závislý na způsobu provozu a četnosti vyžádání bezpečnostní funkce. Rozlišuje se:

- režim s nízkým vyžádáním, kdy provoz systému souvisejícího s bezpečností je vyžadován nejvýše jednou během roku; cílová míra poruch pak vyjadřuje střední pravděpodobnost poruchy plnit na vyžádání požadovanou funkci;
- režim s vysokým nebo nepřetržitým vyžádáním, kdy provoz systému souvisejícího s bezpečností je vyžadován častěji než jednou během roku nebo trvale; cílová míra poruch v tomto případě představuje pravděpodobnost nebezpečné poruchy za hodinu [15].

Hodnoty cílové míry poruch pro jednotlivé úrovně integrity bezpečnosti (SIL) obou uvedených režimů vyžádání bezpečnostní funkce jsou uvedeny v tabulkách č. 3.1 a 3.2.

Tabulka č. 3.1: Cílová míra poruch pro úrovně integrity bezpečnosti v režimu provozu s nízkým vyžádáním

Úroveň integrity bezpečnosti (SIL)	**Cílová míra poruch [-]** (Střední pravděpodobnost poruchy bezpečnostní funkce na vyžádání)
SIL 4	$\langle 10^{-5}, 10^{-4})$
SIL 3	$\langle 10^{-4}, 10^{-3})$
SIL 2	$\langle 10^{-3}, 10^{-2})$
SIL 1	$\langle 10^{-2}, 10^{-1})$

Tabulka č. 3.2: Cílová míra poruch pro úrovně integrity bezpečnosti v režimu provozu s vysokým nebo nepřetržitým vyžádáním

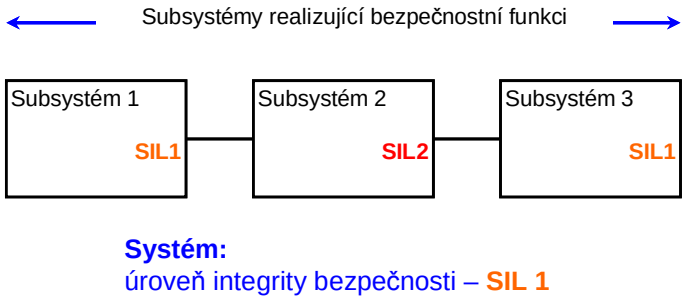
Úroveň integrity bezpečnosti (SIL)	**Cílová míra poruch [h^{-1}]** (Pravděpodobnost nebezpečné poruchy za hodinu)
SIL 4	$\langle 10^{-9}, 10^{-8})$
SIL 3	$\langle 10^{-8}, 10^{-7})$
SIL 2	$\langle 10^{-7}, 10^{-6})$
SIL 1	$\langle 10^{-6}, 10^{-5})$

V technické praxi může být bezpečnostní funkce vykonávána více E/E/PE systémy. Systém související s bezpečností v tomto případě představuje soustavu tvořenou několika subsystémy. Stanovení odpovídající úrovně integrity bezpečnosti (SIL) tohoto systému se provádí využitím přístupu omezení architektury hardware [16].

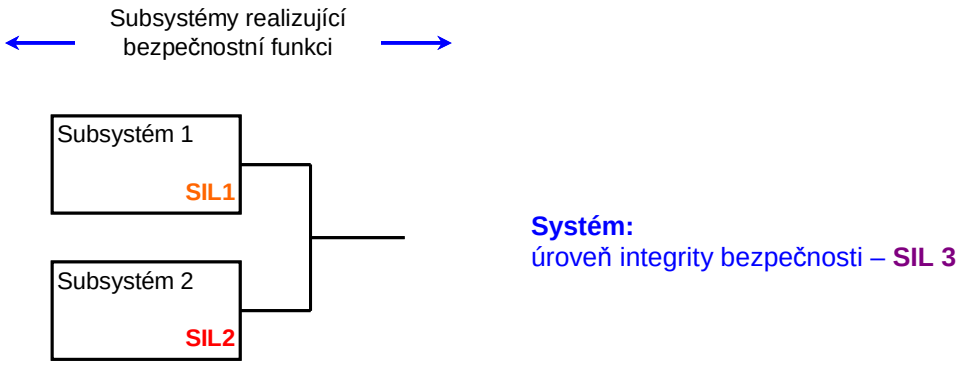
U sériových soustav, kdy je bezpečnostní funkce realizována jediným kanálem, dochází k poruše bezpečnostní funkce při poruše kteréhokoliv subsystému v kanálu. Maximální úroveň integrity bezpečnosti (SIL), které lze u tohoto systému dosáhnout, je omezena nejnižší hodnotou SIL u jednotlivých subsystémů, viz obr. č. 3.3.

U paralelního uspořádání subsystémů vykonávajících bezpečnostní funkci může být bezpečnostní funkce realizována prostřednictvím více kanálů. V případě poruchy subsystémů v určitém kanálu může být bezpečnostní funkce zajištěna subsystémy v ostatních kanálech. Tato redundance při realizaci bezpečnostní funkce je např. pro dvoukanálovou architekturu

hardware vyjádřena zvýšením vyšší úrovně SIL jednotlivých subsystémů o jednu úroveň, viz obr. č. 3.4.



Obr. č. 3.3: Sériové uspořádání subsystémů



Obr. č. 3.4: Paralelní uspořádání subsystémů

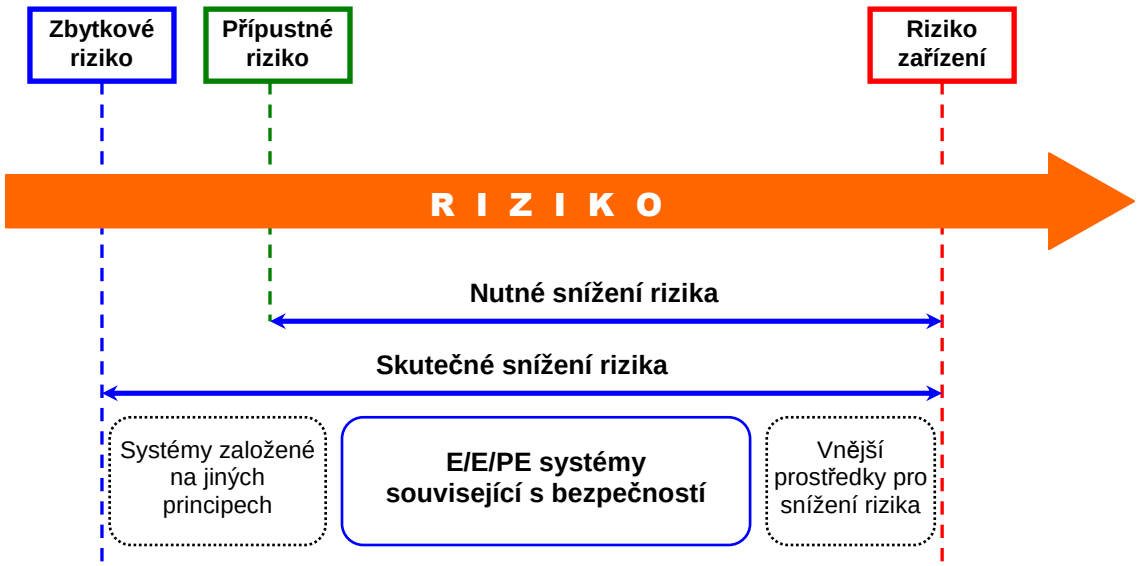
Typické E/E/PE systémy související s bezpečností jsou obvykle tvořeny větším počtem subsystémů. Tyto mohou být reprezentovány subsystémy vstupů (senzorů), subsystémy logických bloků, subsystémy výstupů (akčních členů) apod. v jednokanálovém, případně vícekanálovém uspořádání.

Využitím obou výše uvedených přístupů omezení architektury hardware lze stanovit požadavek na úroveň integrity bezpečnosti systémů souvisejících s bezpečností tvořených libovolným počtem subsystémů v různém uspořádání kanálů zajišťujících bezpečnostní funkci. Postupnou redukcí architektury hardware lze stanovit maximální hodnotu SIL, kterou daný systém související s bezpečností může dosáhnout.

3.2 Kvalitativní hodnocení funkční bezpečnosti

Smyslem systémů souvisejících s bezpečností je snížení rizika řízených zařízení (EUC) na přijatelnou úroveň. Tato úroveň rizika je definována požadovanou úrovní integrity bezpečnosti, které má být pro daný bezpečnostní systém dosaženo. Snížení rizika je u těchto systémů realizováno snížením četnosti nebezpečných událostí a současně zmírněním jejich následků.

Snížení rizika na přípustnou úroveň u řízeného zařízení (EUC), systému řízení EUC a vlivu lidského činitele, založené na principu systémů souvisejících s bezpečností, spočívá ve snížení existujícího rizika (bez předpokladu jakýchkoliv bezpečnostních opatření) minimálně na společensky přijatelnou úroveň. Toho je dosahováno použitím kombinace ochranných prvků, založených na principu E/E/PE systémů souvisejících s bezpečností, systémů založených na jiných technických principech a vnějších prostředků pro snížení rizika, viz obr. č. 3.5.



Obr. č. 3.5: Princip nutného snížení rizika

U E/E/PE systémů souvisejících s bezpečností je snížení rizika na přijatelnou úroveň realizováno prostřednictvím následujících činností [18]:

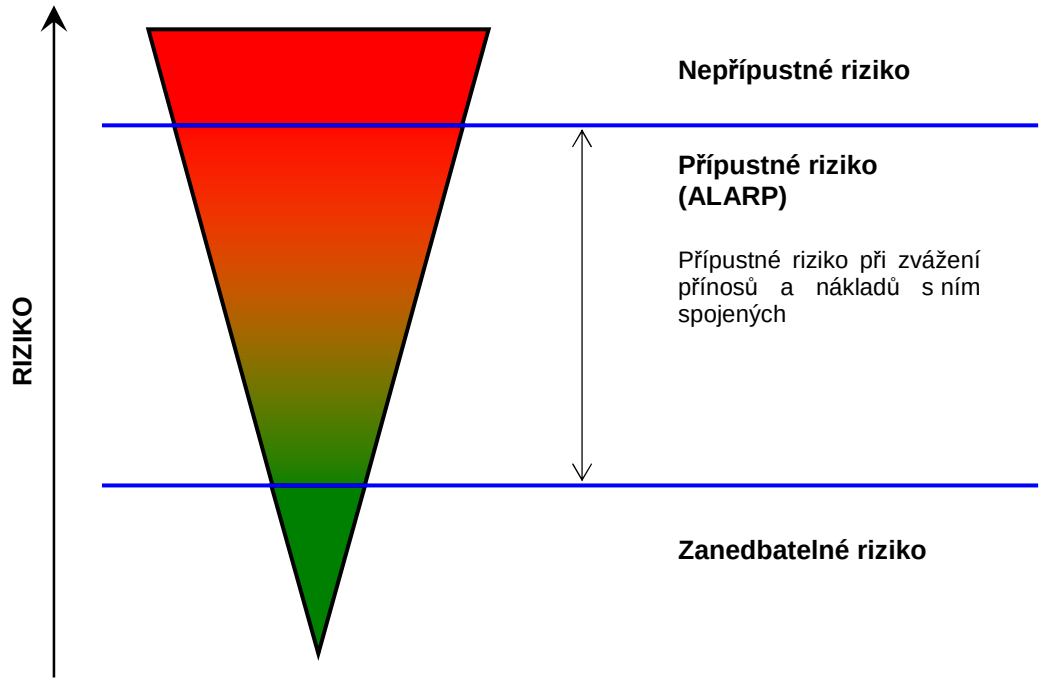
- realizace požadované bezpečnostní funkce nutné pro dosažení nebo udržení bezpečného stavu u řízeného zařízení (EUC),

- dosažení nutné integrity bezpečnosti pro bezpečnostní funkci (samostatně nebo v součinnosti s ostatními bezpečnostními systémy), zajišťující dostatečně nízkou pravděpodobnost nebezpečných událostí a omezení jejich následků.

Pro přiřazení bezpečnostních požadavků systémů souvisejících s bezpečností, tj. bezpečnostních funkcí a úrovně integrity bezpečnosti (SIL), se využívá řada metod, založených na různých principech. Níže jsou popsány vybrané kvalitativní metody pro návrh požadavků vedoucích k nutnému snížení rizika.

3.2.1 Metoda ALARP

Metoda hodnocení rizika ALARP vychází z kategorizace rizika do tří skupin: rizika nepřijatelně velkého, rizika zanedbatelně malého a oblasti rizika vymezeného uvedenými hraničními hodnotami. Právě toto rozmezí představuje oblast ALARP, tj. riziko na nejnižší rozumně proveditelné úrovni, ALARP – as low as reasonably practicable. Cílem této metody je snížení rizika na nejnižší možnou úroveň, s přihlédnutím k přínosům plynoucím z přijetí rizika a k nákladům spojeným se snížením rizika ve vztahu k dosaženému zlepšení bezpečnosti [18]. Princip metody je zobrazen na obr. č. 3.6.



Obr. č. 3.6: Koncepce metody ALARP

Praktickou aplikací koncepce ALARP představuje hodnocení rizika s využitím tříd rizika, vycházející z principu kategorizace možných následků nebezpečných událostí a jejich předpokládané četnosti. Obecný příklad pro čtyři třídy rizika je uveden v tabulce č. 3.3 [18].

Třídy rizika představují úroveň rizika po provedení opatření ke snížení rizika. Pro uvedenou klasifikaci tříd rizika lze rozlišit:

- třída I – nepřípustné riziko,
- třída II – nežádoucí riziko, přípustné pouze v případě, že jeho další snížení je neproveditelné, nebo náklady na jeho snížení jsou neúměrné dosaženému zlepšení bezpečnosti,
- třída III – přípustné riziko v případě, že náklady na jeho snížení jsou neúměrné dosaženému zlepšení bezpečnosti,
- třída IV – zanedbatelné riziko ve všeobecně přijatelné oblasti.

Tabulka č. 3.3: Klasifikace rizika, obecný případ

Četnost	Následek			
	katastrofální	kritický	nepodstatný	zanedbatelný
častá	I	I	I	II
pravděpodobná	I	I	II	III
příležitostná	I	II	III	III
málo častá	II	III	III	IV
nepravděpodobná	III	III	IV	IV
neuvěřitelná	IV	IV	IV	IV

Z koncepce ALARP vycházejí kvantitativní i kvalitativní metody přiřazení bezpečnostních požadavků, které jsou založeny na hodnocení rizik. Příklad kvalitativní metody je uveden v následující kapitole.

3.2.2 Diagram rizika

Metoda diagramu rizika představuje kvalitativní metodu, která umožňuje stanovit úroveň integrity bezpečnosti (SIL) u systémů souvisejících s bezpečností. Je založena na analýze rizika řízeného zařízení (EUC) a systému řízení EUC.

Metoda zavádí několik parametrů, které dohromady charakterizují základní vlastnosti nebezpečné situace v případě selhání systému souvisejícího s bezpečností. Princip metody je založen na rovnici [18]:

$$R = f \cdot C \quad [-] \tag{3.1}$$

kde: R – riziko bez systémů souvisejících s bezpečností,
f – četnost výskytu nebezpečné události bez systémů souvisejících s bezpečností,
C – následek nebezpečné události.

Na základě uvedené rovnice se vyhodnocují následující čtyři parametry rizika:

- následek nebezpečné události (*C*),
- režim vyžádání funkce způsobující nebezpečnou událost (*F*),
- možnost se vyhnout nebezpečné události (*P*),
- pravděpodobnost nežádoucího výskytu (*W*) – bez přidání jakýchkoliv systémů souvisejících s bezpečností, ale s použitím vnějších prostředků pro snížení rizika.

Kategorizace uvedených parametrů rizika je ovlivněna konkrétním řešením řízeného zařízení (EUC), typem prostředí, ve kterém vykonává svou činnost, a vazbami na další systémy a subjekty, u kterých může způsobit ohrožení bezpečnosti. V následujících tabulkách je uveden obecný případ kategorizace parametrů rizika.

Tabulka č. 3.4: Následek nebezpečné události

Následek (C)	C1	menší zranění
	C2	zranění více osob s trvalými následky, smrt jedné osoby
	C3	smrt několika osob
	C4	smrt velkého počtu osob

Tabulka č. 3.5: Režim vyžádání funkce

Režim vyžádání funkce (F)	F1	vzácná a častější doba funkce
	F2	častá až trvalá doba funkce

Tabulka č. 3.6: Možnost se vyhnout nebezpečné události

Možnost se vyhnout nebezpečné události (P)	P1	možné za určitých podmínek
	P2	téměř nemožné

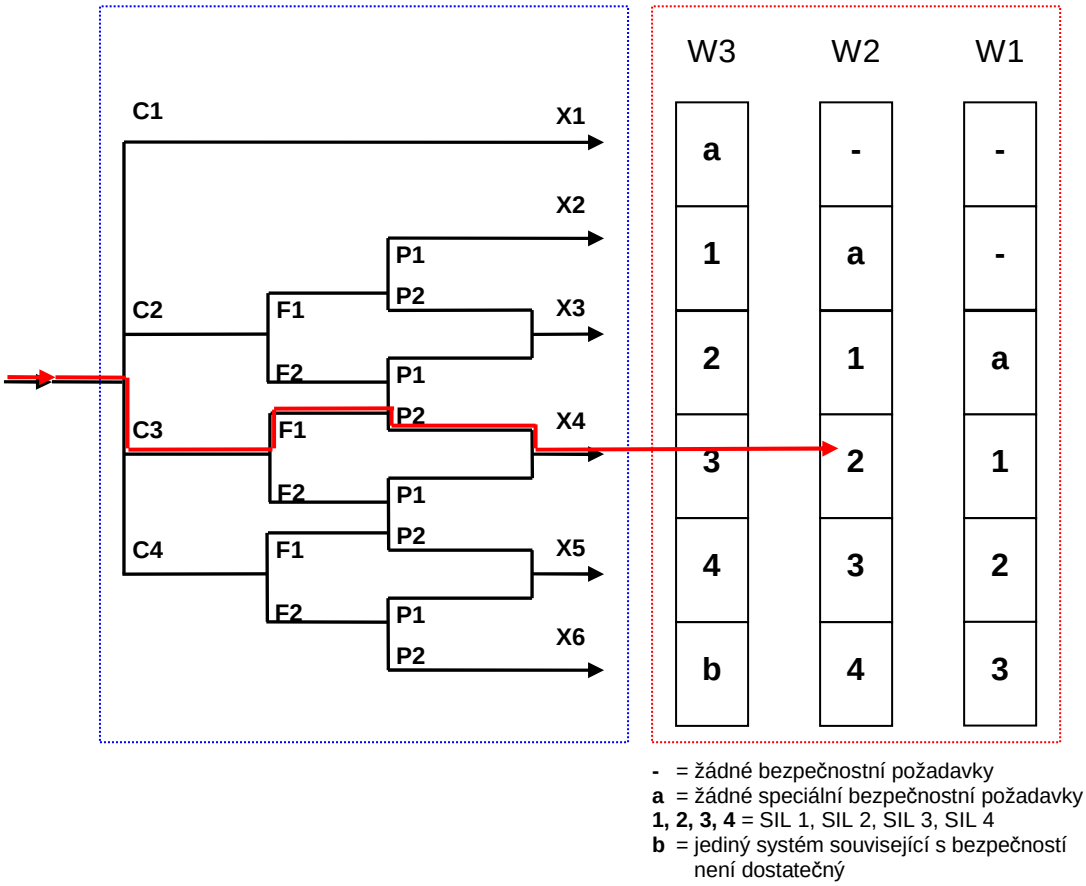
Pro možnost volby P1 (vyhnutí nebezpečné události za určitých podmínek) musí být splněny všechny následující předpoklady:

- upozornění obsluhy vnějšími prostředky, že systém selhal,
- možnost zabránění nebezpečné události,
- dostatečná doba k zabránění nebezpečné události.

Tabulka č. 3.7: Pravděpodobnost nežádoucího výskytu

Pravděpodobnost nežádoucího výskytu (W)	W1	velmi malá
	W2	malá
	W3	poměrně vysoká

Diagram rizika pro výše uvedené vstupní údaje je uveden na obr. č. 3.7. Použití parametrů rizika *C, F, P* vede na jeden z osmi výstupů. Každý z těchto výstupů je mapován do jedné ze tří stupnic (*W1, W2, W3*). Každý stupeň těchto stupnic vyznačuje nutnou integritu bezpečnosti (SIL), kterou musí systém související s bezpečností splňovat.



Obr. č. 3.7: Diagram rizika, určení úrovně integrity bezpečnosti (SIL)

3.3 Kvantitativní hodnocení funkční bezpečnosti

Úroveň integrity bezpečnosti hardware u systémů E/E/PE souvisejících s bezpečností je mimo architektury hardware ovlivněna zejména jejími specifickými kvantitativními ukazateli, tj. diagnostickým pokrytím a cílovou mírou poruch. Tyto hodnoty charakterizují u systémů souvisejících s bezpečností pravděpodobnost náhodných nebezpečných poruch

hardware a možnost jejich včasného odhalení prostřednictvím provádění automatických diagnostických testů systému. Systematické poruchy hardware těchto systémů jsou posuzovány s využitím součinitele účinku společných poruch.

Pro kvantitativní ukazatele funkční bezpečnosti norma ČSN EN 61508 předpokládá během stanovené předpokládané doby života systému E/E/PE konstantní hodnoty intenzit poruch, odpovídající exponenciálnímu rozdělení pravděpodobnosti náhodné veličiny. Výpočty vztahující se k intenzitám poruch těchto systémů by měly být prováděny pro konfidenční úroveň minimálně 70 %.

3.3.1 Diagnostické pokrytí

U systémů E/E/PE souvisejících s bezpečností jsou podle vlivu poruchy na bezpečnostní funkci rozlišovány poruchy nebezpečné, které uvádějí systém související s bezpečností do stavu, kdy nemůže vykonávat svou funkci, a poruchy bezpečné, kdy funkce systému souvisejícího s bezpečností není omezena. Intenzita poruch těchto systémů zahrnuje vliv obou typů poruch, neboli:

$$\lambda = \lambda_D + \lambda_S \qquad [h^{-1}] \qquad (3.2)$$

kde: λ – intenzita poruch systému E/E/PE [h^{-1}],
λ_D – intenzita nebezpečných poruch [h^{-1}],
λ_S – intenzita bezpečných poruch [h^{-1}].

Riziko u systémů souvisejících s bezpečností je tedy vyvoláno vznikem nebezpečných poruch. Nutné snížení rizika těchto systémů pro zachování integrity bezpečnosti je v tomto případě prováděno včasnou detekcí nebezpečných poruch. Za tímto účelem musí být u systémů E/E/PE zajištěno provádění automatických diagnostických testů, které jsou založeny na principu porovnávacích kontrol, standardních zkušebních programů, trvalého monitorování signálů, zkoušek vnějšími podněty apod.

Na základě provádění automatických diagnostických testů se u nebezpečných poruch rozlišují poruchy detekované, zjištěné diagnostickými testy, a poruchy nedetekované, které nejsou diagnostickými testy odhalitelné. Pro intenzity uvedených poruch platí:

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \qquad [h^{-1}] \qquad (3.3)$$

kde: λ_D – intenzita nebezpečných poruch [h^{-1}],
λ_{DD} – intenzita nebezpečných diagnostikovaných poruch [h^{-1}],
λ_{DU} – intenzita nebezpečných nediagnostikovaných poruch [h^{-1}].

Diagnostické pokrytí (DC) vyjadřuje podíl na snížení pravděpodobnosti nebezpečných poruch hardware v důsledku provádění automatických diagnostických testů [17]. Určuje se pro jednotlivé subsystémy související s bezpečností, tvořené jednotlivými součástmi a skupinami součástí, podle vztahu:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} \quad [-] \qquad (3.4)$$

Jsou-li při kategorizaci poruch subsystémů souvisejících s bezpečností zjištěny kromě nebezpečných poruch také poruchy bezpečné, je určován také ukazatel, označovaný jako podíl bezpečných poruch (SFF), daný vztahem:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \quad [-] \qquad (3.5)$$

Hodnota diagnostického pokrytí, resp. podílu bezpečných poruch, ovlivňuje úroveň integrity bezpečnosti jednotlivých subsystémů souvisejících s bezpečností a také uspořádání architektury hardware, které má být pro dosažení požadované funkční bezpečnosti použito.

Požadavky na úroveň integrity bezpečnosti (SIL) pro různé úrovně podílu bezpečných poruch jsou uvedeny v tabulce č. 3.8. Uvedená tabulka vyjadřuje přísnější požadavky pro systémy, které se v technické praxi často vyskytují a pro které ve vztahu k bezpečnostní funkci platí:

- nejsou definovány všechny poruchové režimy systému a jeho součástí, nebo
- nelze plně určit chování systému při vzniku nebezpečné poruchy, nebo
- nejsou k dispozici dostatečně spolehlivé údaje o poruchách systému získané z provozu.

Tabulka č. 3.8: Omezení architektury hardware v souvislosti s integritou bezpečnosti

Podíl bezpečných poruch *SFF* [%]	**Odolnost proti poruchám hardware *N***		
	0	1	2
< 60	nedovolena	SIL 1	SIL 2
60 ÷ 90	SIL 1	SIL 2	SIL 3
90 ÷ 99	SIL 2	SIL 3	SIL 4
≥ 99	SIL 3	SIL 4	SIL 4

Ve výše uvedené tabulce odolnost proti poruchám hardware N znamená, že $N+1$ poruch by způsobilo ztrátu bezpečnostní funkce. Kupříkladu u subsystémů, jejichž hardware je tvořen jedním kanálem, je odolnost proti poruchám hardware $N=0$ (jediná porucha způsobí ztrátu bezpečnostní funkce). Při podílu bezpečných poruch např. v rozsahu $60 \div 90$ % dosahuje subsystém tvořený jedním kanálem úrovně integrity bezpečnosti SIL 1, subsystém tvořený dvěma kanály (paralelní uspořádání) dosahuje úrovně integrity bezpečnosti SIL 2.

Metoda výpočtu diagnostického pokrytí (DC), resp. podílu bezpečných poruch (SFF) pro systémy E/E/PE související s bezpečností vychází z posouzení všech typů poruch a možnosti jejich detekce u jednotlivých prvků, které tvoří posuzovaný systém.

Pro každou součást se provede kategorizace možných poruch a určí se odpovídající intenzita bezpečných a nebezpečných poruch. U nebezpečných poruch se následně provede analýza všech možných způsobů poruch (např. rozpojení obvodu, zkrat obvodu, změna hodnoty signálu apod.) a možnost jejich detekce prováděním automatických diagnostických testů. Pokud není možné analýzou zjistit hodnotu podílu detekovatelných poruch daného prvku, předpokládá se, že 50 % poruch je diagnostikovaných a 50 % poruch nediagnostikovaných.

Na základě analýzy možných způsobů poruch se pro každý prvek určí jeho diagnostické pokrytí a intenzita nebezpečných diagnostikovaných, resp. nediagnostikovaných poruch. Uvedeným postupem se získají pro jednotlivé prvky hodnoty intenzit poruch λ_S, λ_{DD} a λ_{DU}, jejichž dosazením do vztahů (3.4), resp. (3.5) lze získat hodnotu diagnostického pokrytí a podílu bezpečných poruch pro systém související s bezpečností.

3.3.2 Cílová míra poruch

Cílová míra poruch (PFH) představuje základní kvantitativní ukazatel hodnocení funkční bezpečnosti hardware systémů E/E/PE souvisejících s bezpečností v souvislosti se vznikem náhodných poruch. Přístup k výpočtu této hodnoty je závislý na režimu provozu a na architektuře hardware uvedených systémů.

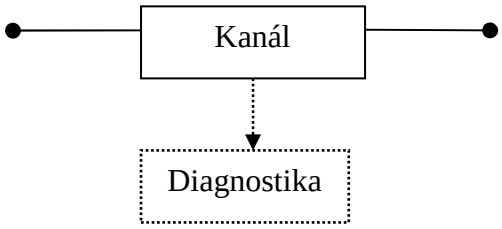
V případě systémů pracujících v režimu provozu s vysokým nebo nepřetržitým vyžádáním představuje cílová míra poruch pravděpodobnost nebezpečné poruchy systému souvisejícího s bezpečností za hodinu [15]. Postup výpočtu pro uvedený případ je uveden níže.

Skutečně nebezpečné poruchy systémů E/E/PE souvisejících s bezpečností představují poruchy, které vedou ke ztrátě bezpečnostní funkce a současně nejsou detekovány prováděním automatických diagnostických testů, tedy nebezpečné nediagnostikované poruchy, jež jsou charakterizovány intenzitou poruch λ_{DU}.

Pro E/E/PE systémy s architekturou hardware tvořenou jedním kanálem (označení 1oo1, viz obr. č. 3.8), odpovídající sériovému uspořádání, se intenzita nebezpečných nediagnostikovaných poruch λ_{DU} kanálu určí podle vztahu (3.6), za předpokladu, že intenzity poruch jsou konstantní, tedy náhodná veličina má exponenciální rozdělení pravděpodobnosti.

$$\lambda_{DU} = \sum_{i=1}^{n} \lambda_{DUi} \qquad [h^{-1}] \qquad (3.6)$$

kde: λ_{DU} – intenzita nebezpečných nediagnostikovaných poruch kanálu [h^{-1}],
λ_{DUi} – intenzita nebezpečných nediagnostikovaných poruch *i*-tého subsystému, resp. skupiny nebo tvořícího prvku [h^{-1}].



Obr. č. 3.8: Architektura 1oo1

Pravděpodobnost nebezpečné nediagnostikované poruchy (PFD) se určí s využitím exponenciálního rozdělení pravděpodobnosti podle vztahu:

$$PFD = 1 - e^{-\lambda_D \cdot t_{CE}} \qquad [-] \qquad (3.7)$$

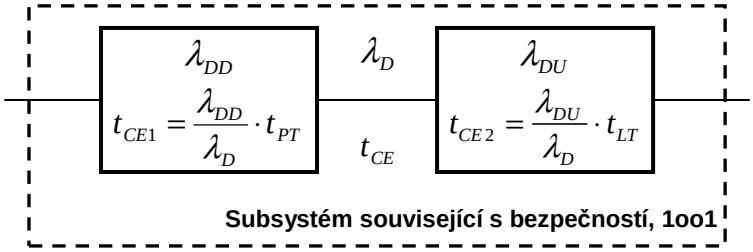
kde: PFD – pravděpodobnost nebezpečné nediagnostikované poruchy kanálu [-],
λ_D – intenzita nebezpečných poruch kanálu [h^{-1}],
t_{CE} – ekvivalentní doba prostoje kanálu [h].

Ve výše uvedeném vztahu doba t_{CE} představuje ekvivalentní dobu prostoje kanálu, tedy dobu, po kterou není systém související s bezpečností schopen vykonávat požadovanou bezpečnostní funkci z důvodu náhodné poruchy hardware. Tato doba je ovlivněna prováděním automatických diagnostických testů a kontrolních periodických zkoušek, které jsou určeny k monitorování správné činnosti systémů souvisejících s bezpečností [19].

V době provozu systému mezi provedením automatických diagnostických testů, případně kontrolními periodickými zkouškami nejsou o činnosti systému souvisejícího

s bezpečností (tedy o dostupnosti bezpečnostní funkce) žádné informace. Vzhledem ke skutečnosti, že některé poruchy se nepodaří detekovat ani uvedenými testy a zkouškami (diagnostické pokrytí nedosahuje ve většině případů 100 %), lze zjistit některé nebezpečné poruchy systémů souvisejících s bezpečností až v případě vyžádání bezpečnostní funkce. V tomto případě místo uvedeného intervalu je nutné pro výpočet zvolit předpokládanou dobu života systému souvisejícího s bezpečností, protože není zřejmé, po jaké době provozu může dojít k vyžádání bezpečnostní funkce, a prostoj kanálu tak může trvat po celou dobu života systému. Tato skutečnost je označována jako účinek nedokonalé kontrolní periodické zkoušky [19].

Pro určení ekvivalentní doby prostoje kanálu t_{CE} je možné vyjádřit subsystém související s bezpečností s architekturou hardware 1oo1 jako sériovou soustavu, tvořenou dvěma pomyslnými bloky, tj. blokem diagnostikovaných poruch a blokem nediagnostikovaných poruch (viz obr. č. 3.9).



Obr. č. 3.9: Pomyslné blokové schéma subsystému 1oo1

Výpočet hodnoty ekvivalentní doby prostoje kanálu t_{CE} je závislý na podílu diagnostikovaných, resp. nediagnostikovaných poruch k celkovému počtu nebezpečných poruch kanálu (dáno podílem příslušných intenzit poruch). Vztah pro výpočet ekvivalentní doby prostoje je dán:

$$t_{CE} = \frac{\lambda_{DD}}{\lambda_D} \cdot t_{PT} + \frac{\lambda_{DU}}{\lambda_D} \cdot t_{LT} \quad [\text{h}] \tag{3.8}$$

kde: t_{CE} – ekvivalentní doba prostoje kanálu [h],
λ_{DD} – intenzita nebezpečných diagnostikovaných poruch [h^{-1}],
λ_{DU} – intenzita nebezpečných nediagnostikovaných poruch [h^{-1}],
λ_D – intenzita nebezpečných poruch [h^{-1}],
t_{PT} – interval mezi diagnostickými testy nebo kontrolními zkouškami [h],
t_{LT} – doba stanovené životnosti systému souvisejícího s bezpečností [h].

V případě, že řízené zařízení (EUC) a systém řízení EUC je v činnosti po dobu obnovy systému souvisejícího s bezpečností (po vzniku náhodné poruchy), je nutné ekvivalentní dobu prostoje kanálu rozšířit také o dobu jeho obnovy, po kterou rovněž není bezpečnostní funkce dostupná.

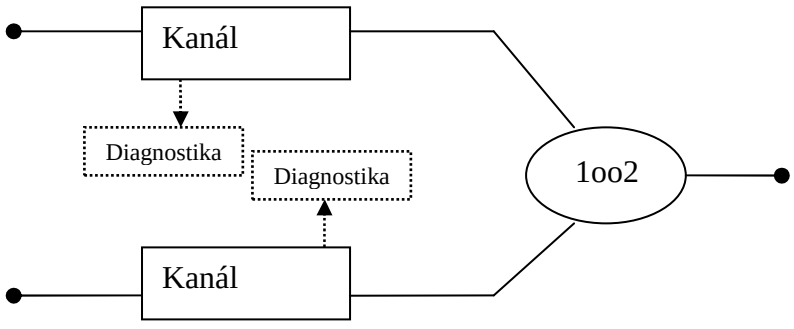
Pokud jsou pro jednokanálovou architekturu systému souvisejícího s bezpečností (1oo1) určeny hodnoty ukazatelů podle výše uvedených vztahů, lze pro tento systém určit cílovou míru poruch (*PFH*) následovně:

$$PFH = \frac{PFD}{t_{LT}} \qquad [h^{-1}] \qquad (3.9)$$

kde: PFH – cílová míra poruch, pro systém s vysokým nebo nepřetržitým vyžádáním [-],
PFD – pravděpodobnost nebezpečné poruchy kanálu [-],
t_{LT} – doba stanovené životnosti systému souvisejícího s bezpečností [h].

Hodnota cílové míry poruch systémů souvisejících s bezpečností je ovlivněna ve značné míře uspořádáním architektury hardware, tj. počtem kanálů vykonávajících bezpečnostní funkci a souvisejícími diagnostickými prostředky. U systémů E/E/PE je uspořádání hardware řešeno obvykle použitím následujících přístupů [19]:

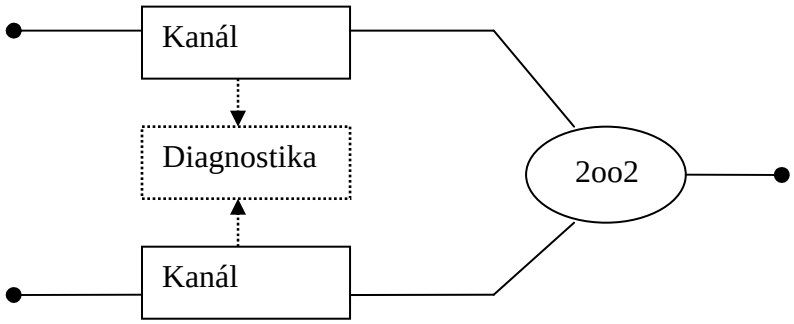
- Architektura 1oo1 – hardware je uspořádán v jediném kanále, přičemž jakákoliv nebezpečná porucha vyvolá ztrátu bezpečnostní funkce.
- Architektura 1oo2 – hardware je uspořádán ve dvou paralelně spojených kanálech, přičemž bezpečnostní funkci může vykonávat nezávisle každý z uvedených kanálů. Ztráta bezpečnostní funkce nastává při nebezpečné poruše v obou kanálech. Diagnostika tohoto systému nemá vliv na rozhodovací logiku výstupních signálů.



Obr. č. 3.10: Architektura 1oo2

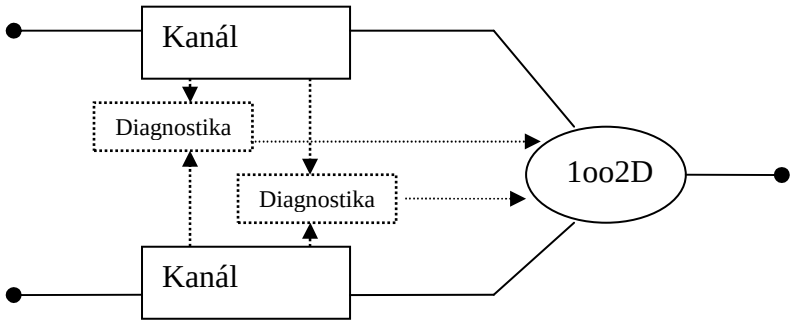
- Architektura 2oo2 – hardware je uspořádán ve dvou paralelně spojených kanálech, přičemž bezpečnostní funkci mohou vykonávat pouze oba kanály současně. Ztráta

bezpečnostní funkce tak nastává při nebezpečné poruše kteréhokoliv kanálu. Diagnostika tohoto systému nemá vliv na rozhodovací logiku výstupních signálů.



Obr. č. 3.11: Architektura 2oo2

- Architektura 1oo2D – hardware je uspořádán ve dvou paralelně spojených kanálech. Při běžném provozu je bezpečnostní funkce vykonávána oběma kanály současně. Je-li diagnostickými testy zjištěna nebezpečná porucha v jednom z kanálů, uzpůsobí se rozhodovací logika výstupních signálů tak, že bezpečnostní funkci vykonává pouze druhý kanál. Ztráta bezpečnostní funkce nastane v případě, že dojde k nebezpečné poruše i ve druhém kanále.



Obr. č. 3.12: Architektura 1oo2D

Pro potvrzení celkové bezpečnosti systémů souvisejících s bezpečností v souladu s požadavky normy ČSN EN 61508, tedy zda splňují požadovanou úroveň integrity bezpečnosti (SIL), je nutné realizovat zkoušky a testování. Skutečnou hodnotu parametru náhodných poruch hardware, tj. cílovou míru poruch, je nutné ověřit provedením zkoušek spolehlivosti. Této tematice je věnována následující kapitola.

4 ZKOUŠKY SPOLEHLIVOSTI

Kvalita každého výrobku se plně projeví až v průběhu jeho dlouhodobého provozu. Dostačující nejsou pouze jeho technické parametry, ale také odpovídající úroveň jeho provozní spolehlivosti.

Aby bylo možné objektivně posoudit skutečnou spolehlivost těchto výrobků, je u nich nutné provést zkoušku spolehlivosti. Tímto postupem lze ověřit informace o spolehlivosti výrobků, které byly určeny analytickými metodami, tedy vyplývající z teoretického modelu spolehlivosti, a tím provést jejich potvrzení nebo zamítnutí. V případě, kdy nejsou použity prediktivní metody pro zjištění parametrů spolehlivosti, se zkoušky spolehlivosti využívají k přímému experimentálnímu stanovení parametrů spolehlivosti zkoušených výrobků.

Tyto zkoušky jsou obvykle prováděny na omezeném množství výrobků a často ve zvláštních podmínkách. Informace získané těmito zkouškami jsou pak exaktními postupy zpracovány, zhodnoceny a zobecněny pro celou populaci vyrobených výrobků. Cílem výrobců, pro zachování konkurenceschopnosti výrobků na trhu, je provedení těchto zkoušek v nejkratším možném čase a při nejnižších možných nákladech, současně při zachování vysoké věrohodnosti dosažených výsledků. V praxi se tak používá řada metod, vedoucích ke snížení počtu zkoušených výrobků, zkrácení průběhu zkoušek nebo zrychlení mechanismu vzniku poruch.

4.1 Provozní zkoušky spolehlivosti

Má-li výrobce nebo provozovatel zařízení dostatečné množství důvěryhodných informací o jeho spolehlivosti, které jsou získány z jeho provozu nebo na základě dědičnosti konstrukce, je vhodné provést zkoušku spolehlivosti tohoto zařízení jako zkoušku provozní s využitím uvedených dat. Určení nebo ověření sledovaných parametrů spolehlivosti je možné provést s využitím tzv. zkušebních plánů, které stanovují podmínky provedení zkoušky spolehlivosti a postup jejího vyhodnocení.

4.1.1 Zkušební plány

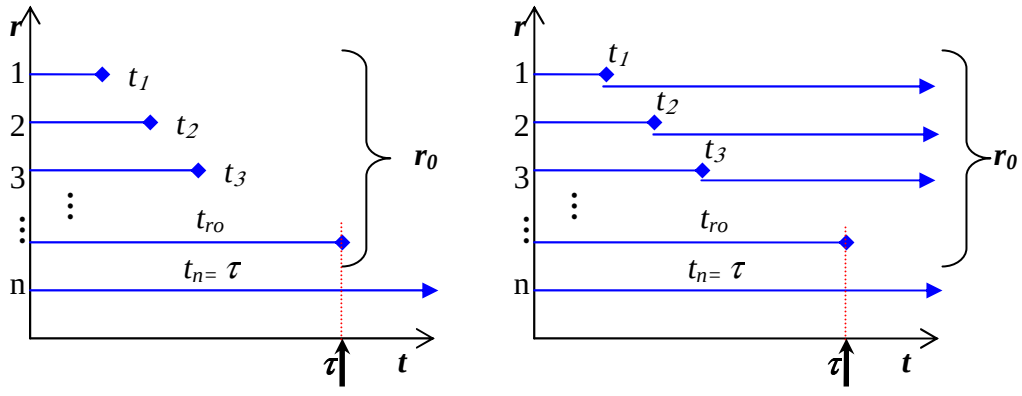
V technické praxi není většinou možné realizovat zkoušky spolehlivosti u všech vyrobených objektů, a to z důvodů ekonomických, časových, ale i proto, že řada zkoušek je

destrukční. Z praktických důvodů je tedy nutné se omezit na zkoušení vhodně vybrané skupiny objektů (zkušební vzorek) a z výsledků jeho zkoušek usuzovat na vlastnosti všech vyráběných objektů (základní soubor). Při shromažďování údajů pro odhady ukazatelů se musí postupovat podle pevných pravidel, jejichž souhrn se nazývá zkušební plán [7].

Pro zkušební plány se používá označení sestávající z kombinace tří symbolů, uzavřených do hranatých závorek. Na prvním místě je uveden počet zkoušených objektů *n*. Na druhém místě jsou symboly *U*, *R* nebo *M* podle způsobu nahrazování objektu po jeho poruše v průběhu zkoušky. Na třetím místě je buď symbol *r* (zkouška se ukončí při výskytu *r*-té poruchy, přitom $r = 0, 1, 2, 3, ..., n$) nebo *t* (zkouška se ukončí po uplynutí předepsané doby τ).

Každá zkouška spolehlivosti se realizuje s n_i výrobky ($i = 1, 2, \dots, n$). Zkouška končí buď po určité době trvání $t = \tau_0$, nebo po vzniku určitého počtu poruch $r = r_0$. Lze tedy rozlišit dvě základní skupiny zkušebních plánů [7]:

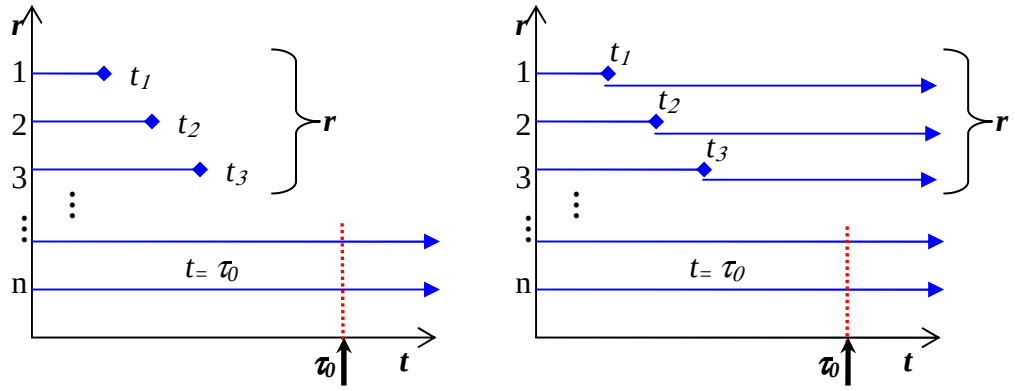
- *r* – plány – do zkoušky je zařazeno n_i stejných výrobků. Zkouška končí po nastoupení předem daného počtu poruch $r = r_0$. Porušené prvky se v průběhu zkoušky buď nahrazují novými $[n, R, r_0]$, nebo nenahrazují $[n, U, r_0]$, nebo se opravují $[n, M, r_0]$. Náhodnou veličinou je doba trvání zkoušky $t = \tau$. Soubor údajů, získaných pomocí tohoto typu zkušebních plánů, se označuje jako jednoduše cenzurovaný soubor I. typu (cenzurovaný počtem poruch). Grafické znázornění tohoto zkušebního plánu je na obr. č. 4.1.



[*n, U, r*$_0$] **[*n, R, r*$_0$]** a **[*n, M, r*$_0$]**

Obr. č. 4.1: Znázornění zkušebních plánů: r – plány

- t – plány – do zkoušky je zařazeno n_i stejných výrobků. Zkouška končí po uplynutí předem dané doby zkoušení $t = \tau_0$. Porušené prvky se v průběhu zkoušky buď nahrazují novými [n, R, τ_0], nebo se nenahrazují novými [n, U, τ_0] nebo se po poruše opravují [n, M, τ_0]. Náhodnou veličinou je počet poruch r, který nastane po dobu trvání zkoušky. Soubor údajů, získaný pomocí tohoto typu zkušebních plánů, se označuje jako jednoduše cenzurovaný soubor II. typu (cenzurovaný dobou trvání zkoušky). Grafické znázornění tohoto zkušebního plánu je uvedeno na obr. č. 4.2.



[n, U, τ_0] **[n, R, τ_0]** a **[n, M, τ_0]**

Obr. č. 4.2: Znázornění zkušebních plánů: t – plány

Cílem zkoušek spolehlivosti je odhad parametrů spolehlivosti, které reprezentují nejen vybraný zkušební soubor, ale všechny vyrobené výrobky, tedy celou populaci. Pro tyto účely se parametr spolehlivosti určuje jako intervalový odhad na zvolené konfidenční úrovni C, ve kterém se nachází skutečný parametr populace s vysokou, předem stanovenou pravděpodobností.

Vzhledem ke skutečnosti, že u zkoušek spolehlivosti podle zkušebních plánů se vyskytují cenzurované soubory dat, nelze pro ně jednoznačně určit typ rozdělení pravděpodobnosti náhodné veličiny. Z tohoto důvodu nelze pro odhad parametrů spolehlivosti použít běžné metody intervalového odhadu. Lze však dokázat [7], že pro vztah parametru spolehlivosti získaného výběru (zkušebního souboru) a parametru spolehlivosti základního souboru (populace) existuje statistika, pro kterou platí, že má chí-kvadrát rozdělení pro zadanou konfidenční úroveň C a počet stupňů volnosti $2r$. Pro pravděpodobnost platí:

$$P\left(\chi^2_{2\nu;\,\alpha/2} \le 2\nu \cdot \frac{\hat{\theta}}{\theta} \le \chi^2_{2\nu;\,1-\alpha/2}\right) = C = 1-\alpha \qquad [-] \qquad (4.1)$$

kde: $\hat{\theta}$ – parametr spolehlivosti zkušebního souboru [h],
θ – parametr spolehlivosti populace [h],
C – konfidenční úroveň [-],
α – hladina významnosti [-],
χ^2 – hodnota chí-kvadrát rozdělení [-].

Z uvedeného vztahu lze odvodit rovnice jak pro určení oboustranného konfidenčního intervalu (ohraničeného dolní a horní mezí), tak i jednostranného odhadu parametru spolehlivosti.

Při odhadu parametrů spolehlivosti s využitím zkušebních plánů se hledaný parametr spolehlivosti obvykle určuje jako levostranný konfidenční interval, kdy je pro daný parametr spolehlivosti vypočtena pouze dolní mez. Pak s pravděpodobností C je hodnota parametru spolehlivosti základního souboru (populace) rovna nebo větší než dolní mez intervalu.

Pro exponenciální rozdělení pravděpodobnosti dob do poruchy se dolní mez T_D konfidenčního intervalu, představujícího intervalový odhad střední doby do poruchy, určí podle vztahu:

$$T_D \ge \frac{2 \cdot t_{AKU}}{\chi^2_{2\nu;C}} \qquad [\mathrm{h}] \qquad (4.2)$$

V uvedeném vztahu (4.2) představuje člen t_{AKU} [h] akumulovanou pracovní dobu výrobků zařazených do zkoušky. Jeho hodnota se určí jako součet doby činnosti všech výrobků po dobu zkoušky (do vzniku poruchy nebo do ukončení zkoušky, pokud porucha nevznikne), neboli:

$$t_{AKU} = \sum_{i=1}^{r} t_i + (n-r)\cdot\tau \qquad [\mathrm{h}] \qquad (4.3)$$

kde: t_{AKU} – akumulovaná pracovní doba výrobků ve zkoušce [h],
t_i – doba do poruchy i-tého výrobku [h],
n – počet výrobků zařazených do zkoušky [-],
r – počet poruch výrobků při zkoušce [-],
τ – doba trvání zkoušky [h].

Hodnota chí-kvadrát rozdělení ve vztahu (4.2) se určí pro konfidenční úroveň C a počet stupňů volnosti 2ν, který je funkcí počtu poruch zkoušených výrobků r:

$$2\nu = 2 \cdot (r+1) \qquad [-] \qquad (4.4)$$

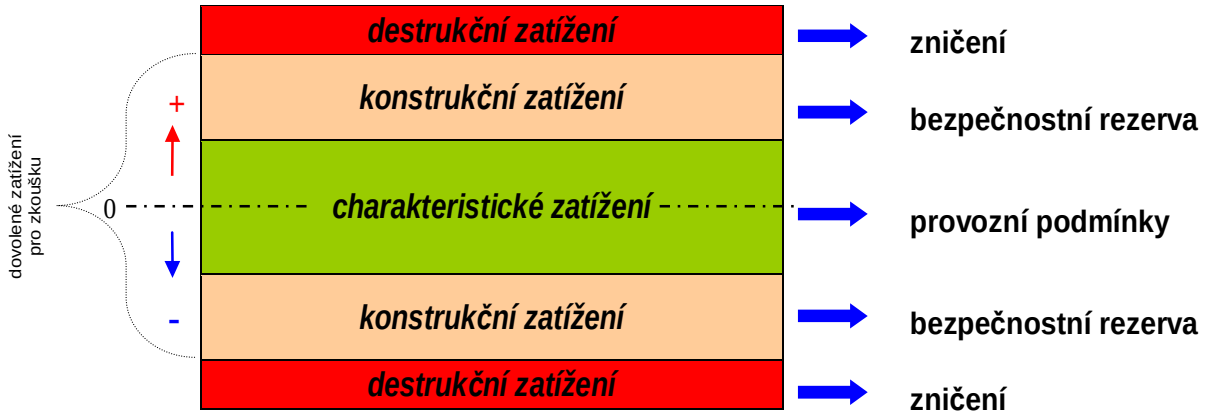
V zájmu zachování konkurenceschopnosti výrobků na trhu je zájmem výrobce provedení zkoušek spolehlivosti během co nejkratší doby. Z přístupu využívající zkušební plány vyplývá, že zkrácení zkoušky se dosáhne zvýšením počtu výrobků zařazených do zkoušky. Další způsoby zrychlení zkoušek spolehlivosti jsou uvedeny v následující kapitole.

4.2 Zrychlené zkoušky spolehlivosti

U mnoha systémů, výrobků nebo součástí se předpokládá jejich bezporuchová činnost po dlouhou dobu v řádu let. Aby bylo možné získat informace o skutečné úrovni spolehlivosti těchto systémů, je nutné provést zkoušku jejich spolehlivosti. Z důvodu nutnosti získání dat o dobách do poruchy výrobků a z důvodu zachování konkurenceschopnosti na trhu, musí být doba provádění zkoušky značně kratší než očekávaná doba života výrobku.

Pro výrobky s velmi vysokou nebo nepřetržitou dobou provozu se musí v průběhu zkoušky spolehlivosti stimulovat vznik poruchy. Provádí se přivedením překračujícího zatížení, vyššího než je zatížení výrobku při normálních provozních podmínkách. Data o dobách do poruchy, získaná za těchto podmínek, jsou pak extrapolována pro provozní podmínky. Tyto zkoušky spolehlivosti mohou být prováděny při vysoké nebo nízké teplotě, vlhkosti, napětí, tlaku, vibracích atd., nebo při kombinaci těchto zatížení.

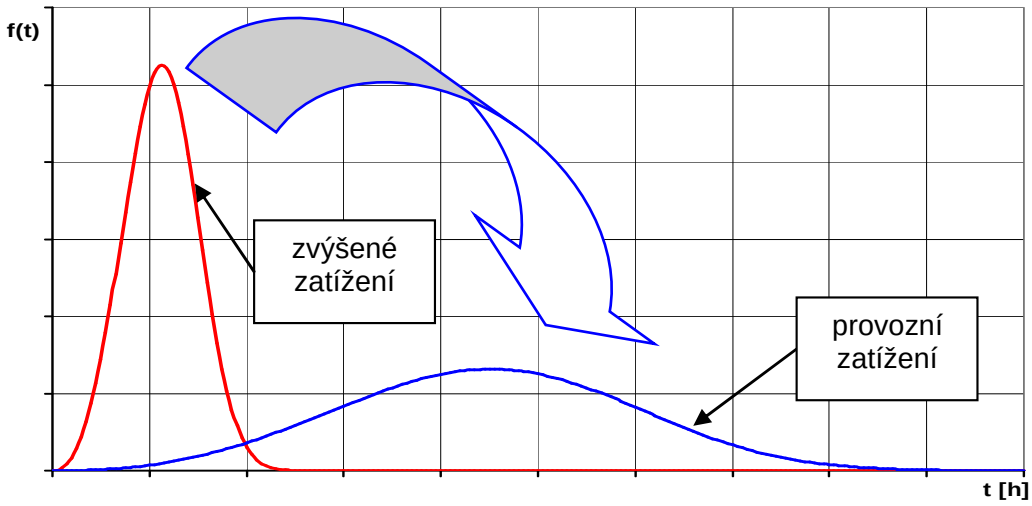
Při zrychlených zkouškách spolehlivosti musí být zvoleny druh a úroveň zatížení tak, aby se zrychlil proces těch poruch, které se vyskytují při provozním zatížení. Zrychlující zvýšené zatížení by nemělo vyvolat poruchy, které se v běžných provozních podmínkách nikdy nevyskytují (viz úrovně zatížení na obr. č. 4.3) [13].



Obr. č. 4.3: Úrovně zatížení výrobku

Volba druhu a úrovně zatížení má nejvyšší význam při plánování zrychlené zkoušky. Návrh zrychlené zkoušky musí být posuzován s ohledem na konstrukci výrobku a použité materiály tak, aby bylo možné určit stimulující zatížení a meze zvýšené úrovně zatížení.

Cílem prováděných zkoušek spolehlivosti je na základě získaných dat zjistit konkrétní charakteristiky spolehlivosti výrobku, jako střední hodnota, intenzita poruch, funkce bezporuchovosti apod., tedy zjistit průběh a konkrétní parametry rozdělení pravděpodobnosti dob do poruchy. Průběh tohoto rozdělení popsaný např. funkcí hustoty pravděpodobnosti se při provozním zatížení a zvýšeném zatížení liší (viz obr. č. 4.4). Musí tak být známa metoda převodu výsledků ze zkoušky při zvýšeném zatížení na běžné provozní podmínky [13].



Obr. č. 4.4: Průběh hustoty pravděpodobnosti pro provozní a zvýšené zatížení

Pro běžně prováděné zrychlené zkoušky spolehlivosti se využívají následující modely závislosti doby života na zatížení, pro převod výsledků na normální provozní zatížení [9]:

- Arrheniův model,
- Eyringův model,
- model inverzní mocninné křivky,
- teplotně-netepelný model,
- teplotně-vlhkostní model,
- model více proměnných,
- model časově proměnného zatížení.

4.2.1 Arrheniův model

Arrheniův model závislosti doby života výrobku na zatížení je nejčastěji používaný vztah při provádění zrychlených zkoušek spolehlivosti v případech, kde zrychlující zatížení ke stimulaci poruchy má tepelný charakter. Je odvozen z Arrheniovy rovnice rychlosti reakce [9]:

$$G(T) = A \cdot e^{-\frac{E_A}{K \cdot T}} \tag{4.5}$$

kde: $G(T)$ – rychlost reakce,
A – netepelná konstanta,
E_A – aktivační energie [eV],
K – Boltzmanova konstanta ($8{,}617385.10^{-5}$ eV.K^{-1}),
T – absolutní teplota [K].

Aktivační energie je energie, kterou musí molekula mít, aby se mohla účastnit reakce, tedy míra vlivu teploty na reakci.

Arrheniův model závislosti doby života na zatížení je formulován za předpokladu, že doba života je úměrná obrácené hodnotě rychlosti reakce v procesu, tedy:

$$L(T) = C \cdot e^{\frac{B}{T}} \quad [\text{h}] \tag{4.6}$$

kde: $L(T)$ – kvantitativní ukazatel spolehlivosti, např. střední hodnota, medián, kvantil,
T – úroveň zatížení (absolutní teplota [K]),
C, B – parametry modelu, které musí být určeny.

V případech, kdy zvýšené zatížení je výlučně tepelné, lze parametr modelu B určit:

$$B = \frac{E_A}{K} \tag{4.7}$$

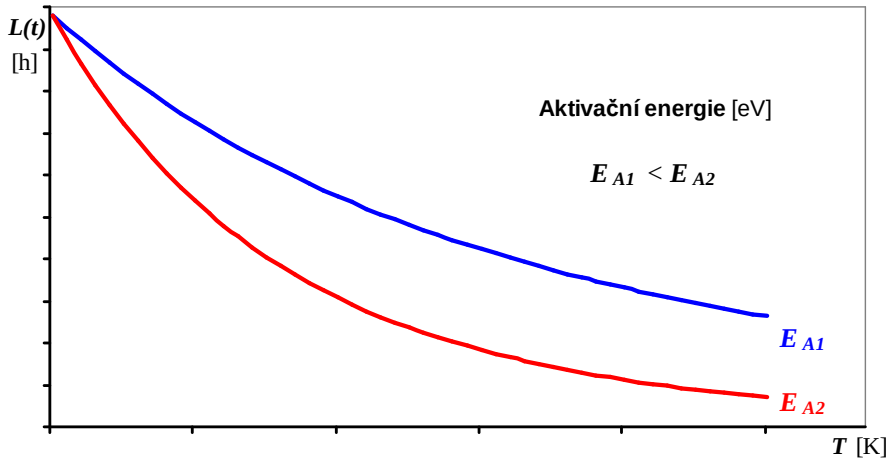
kde: E_A – aktivační energie [eV],
K – Boltzmanova konstanta ($8{,}617385.10^{-5}$ eV.K^{-1}).

Faktor zrychlení, udávající poměr hodnot ukazatele spolehlivosti při provozním zatížení a vyšším zatížení při zrychlené zkoušce, je pro Arrheniův model:

$$A_F = \frac{L_U}{L_A} = \frac{C \cdot e^{\frac{B}{T_U}}}{C \cdot e^{\frac{B}{T_A}}} = e^{B \cdot \left(\frac{1}{T_U} - \frac{1}{T_A}\right)} \quad [-] \tag{4.8}$$

kde: A_F – faktor zrychlení,
L_U – hodnota ukazatele spolehlivosti při provozním zatížení [h],
L_A – hodnota ukazatele spolehlivosti při zvýšeném zatížení [h],
T_U – úroveň zatížení při provozních podmínkách (absolutní teplota [K]),

T_A – zvýšená úroveň zatížení při zkoušce (absolutní teplota [K]),
C, B – parametry modelu.



Obr. č. 4.5: Arrheniův model – závislost parametru spolehlivosti na teplotě

Pro možnost určení faktoru zrychlení zkoušky je nutné znát předem parametr modelu *B*, resp. aktivační energii. V praxi se aktivační energie E_A určuje vyhodnocením dob do poruchy skupin identických součástí zkoušených při různých teplotách, nebo je pro jednotlivé typy součástí uváděna v katalozích výrobků.

4.2.2 Teoretický model pro zrychlené zkoušky systémů

V technické praxi jsou výrobky, včetně elektronických systémů, složeny z velkého množství součástí. Pro možnost ověření nebo určení kvantitativních ukazatelů spolehlivosti těchto systémů je nutné provedení zkoušky spolehlivosti. U elektronických systémů je žádoucí provádět zkoušky spolehlivosti pro výrobek jako celek, kdy jsou zachovány vazby mezi jednotlivými prvky a průběh zkoušky se blíží běžným provozním podmínkám, než kdyby zkouška spolehlivosti probíhala pro každý prvek samostatně.

Zrychlené zkoušky spolehlivosti se avšak v praxi obvykle provádějí pro každý prvek samostatně. Aby bylo možné provést tuto zkoušku pro zařízení jako celek, je nutné vytvořit matematický model pro vyhodnocení výsledků zkoušky a jejich extrapolaci na běžné provozní podmínky daného systému. Níže je provedeno odvození matematického modelu pro zrychlené zkoušky spolehlivosti soustav, vycházející z Arrheniova převodního vztahu. Model je proveden ve dvou variantách podle dostupnosti požadovaných informací o jednotlivých prvcích systému, které jsou potřebné pro vyhodnocení těchto zkoušek spolehlivosti.

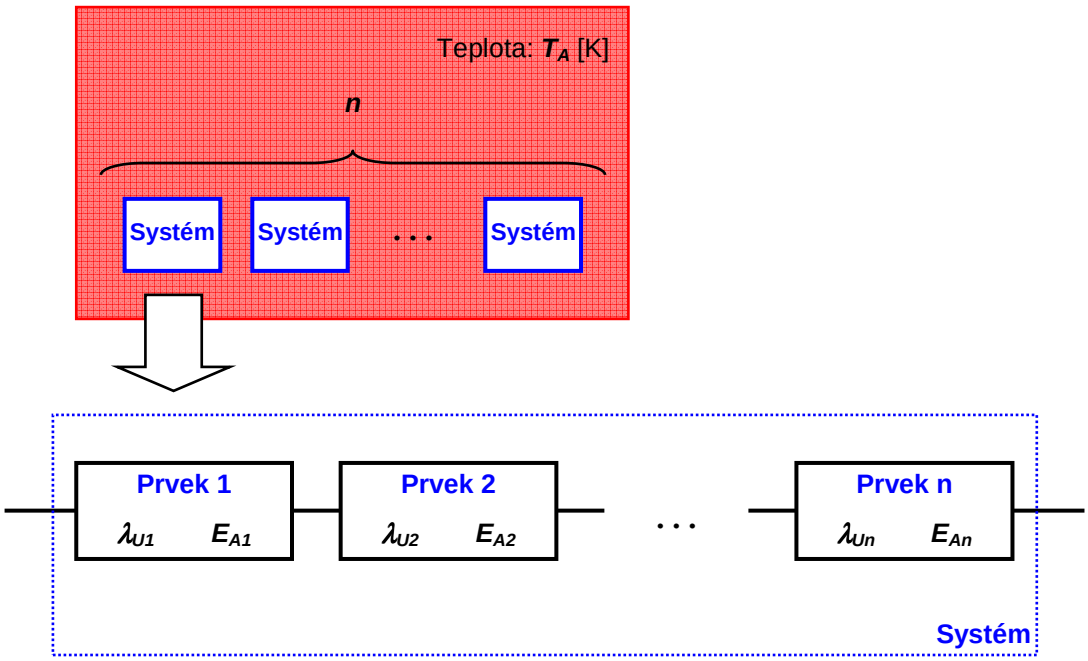
Arrheniův model zkoušky při znalosti aktivační energie prvků

Pro zrychlenou zkoušku spolehlivosti elektronických systémů je vhodné využít Arrheniův model zrychlení zkoušky, kdy zkouška spolehlivosti probíhá při vyšší teplotě než je provozní teplota výrobku.

Pro převod zjištěných kvantitativních ukazatelů spolehlivosti získaných při zrychlené zkoušce $L(T_A)$ na ukazatele odpovídající provozním podmínkám $L(T_U)$ je nutné znát hodnotu faktoru zrychlení zkoušky A_F, viz vztah (4.8).

Aby bylo možné provést zkoušku spolehlivosti pouze při jedné úrovni zvýšené teploty pro n zkoušených výrobků, je nutné znát aktivační energie pro jednotlivé mechanismy vzniku poruch tvořících prvků systému.

Teoretický model spolehlivosti předpokládá, že v blokovém diagramu bezporuchovosti má elektronický systém sériové uspořádání tvořících prvků. Porucha systému tak nastává v případě poruchy kteréhokoliv tvořícího prvku. Každý prvek má známou hodnotu aktivační energie E_A pro předpokládané mechanismy vzniku jeho poruch. Prvky mají v modelu exponenciální rozdělení pravděpodobnosti dob do poruchy, charakterizované intenzitou poruch λ_i, viz obr. č. 4.6.



Obr. č. 4.6: Schéma zkoušky, blokový diagram bezporuchovosti systému

Při vzniku poruchy prvku, která způsobí poruchu systému, je faktor zrychlení závislý na tom, u kterého prvku a jakým způsobem porucha vznikla. Kvantitativní ukazatel spolehlivosti představuje doba do poruchy t_i i-tého systému zařazeného do zkoušky. Přepočet z podmínek zrychlené zkoušky (A) na provozní podmínky (U) se provede podle vztahu:

$$t_{Ui} = e^{\frac{E_{Ai}}{K}\cdot\left(\frac{1}{T_U}-\frac{1}{T_A}\right)} \cdot t_{Ai} \qquad [\text{h}] \qquad (4.9)$$

U modelu zrychlené zkoušky je uvažován zkušební plán [n, U, r], který předpokládá, že pro zkoušku je k dispozici n výrobků, které se po poruše nenahrazují a zkouška končí vznikem r poruch. Pokud vlivem omezení doby trvání zkoušky nevznikne porucha všech výrobků, pak se tyto výrobky do zkoušky nezařazují.

Určení kvantitativního ukazatele spolehlivosti systému je vyjádřeno jako jednostranný intervalový odhad s využitím chí-kvadrát rozdělení. Dolní mez tohoto intervalu T_D pro konfidenční úroveň C se určí ze získaných dob do poruchy, přepočítaných pro provozní podmínky, dle vztahu:

$$T_D \geq \frac{2\cdot\sum_{i=1}^{r} t_{Ui}}{\chi^2_{2(r+1);C}} \qquad [\text{h}] \qquad (4.10)$$

Výsledek zkoušky lze interpretovat např. pro konfidenční úroveň $C = 0{,}9$ tak, že střední doba do poruchy základního souboru, tj. všech vyrobených výrobků, je s pravděpodobností 90 % rovna anebo větší než vypočtená hodnota dolní meze T_D.

Intervalový odhad intenzity poruch elektronického systému při provozních podmínkách λ_U se určí s využitím vztahu pro exponenciální rozdělení [20]:

$$\lambda_U \leq \frac{1}{T_D} \qquad [\text{h}^{-1}] \qquad (4.11)$$

Arrheniův model zkoušky bez znalosti aktivační energie prvků

Arrheniův model pro zrychlenou zkoušku spolehlivosti je možné využít i v případě, že nejsou známy aktivační energie všech prvků nebo všech mechanismů vzniku poruch. Faktor zrychlení A_F, udávající poměr kvantitativních ukazatelů spolehlivosti $L(T_U)$ při provozních podmínkách a ukazatelů při zkušebních podmínkách $L(T_A)$, je pak dán vztahem:

$$A_F = \frac{L(T_U)}{L(T_A)} = e^{B\cdot\left(\frac{1}{T_U}-\frac{1}{T_A}\right)} \qquad [-] \qquad (4.12)$$

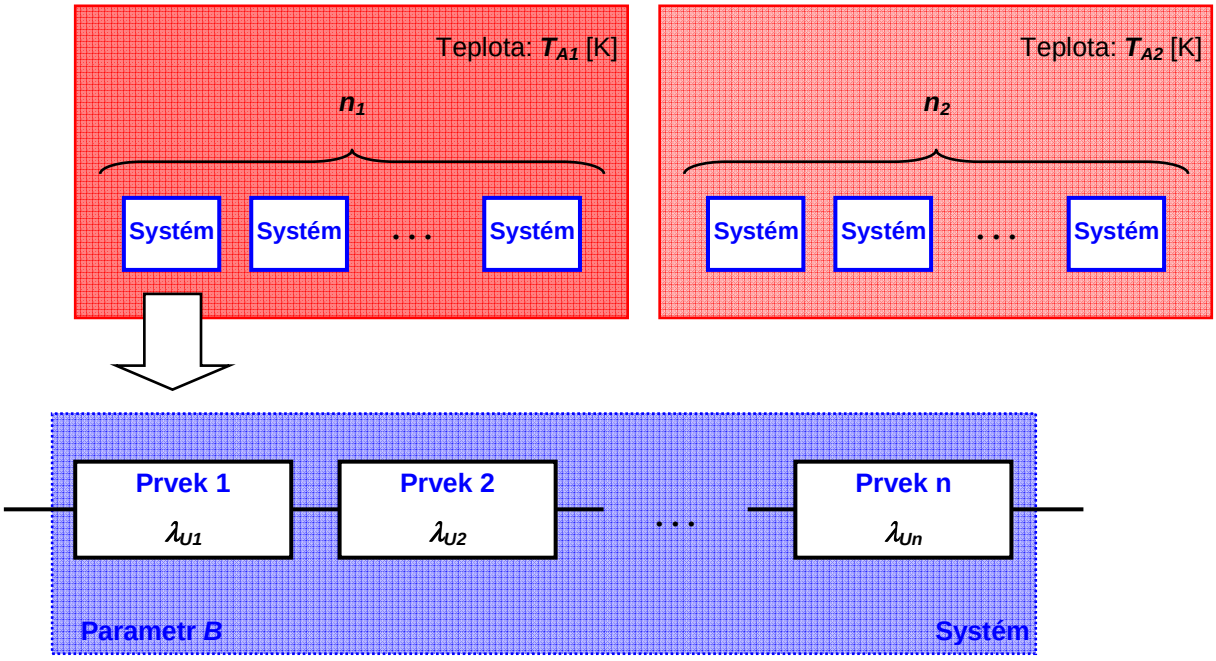
kde: T_U – provozní teplota [K],
T_A – zvýšená teplota při zkoušce [K],
B – neznámý parametr modelu [K],

Neznámý parametr modelu zrychlené zkoušky B je možné určit provedením zkoušky spolehlivosti při dvou různých hodnotách zvýšené teploty, T_{A1} a T_{A2}. Hodnota parametru B se určí s využitím pomocného faktoru zrychlení $\overline{A}_F$ pro kvantitativní ukazatele spolehlivosti při teplotách T_{A1} a T_{A2}, tedy:

$$\overline{A}_F = \frac{L(T_{A2})}{L(T_{A1})} = e^{B\cdot\left(\frac{1}{T_{A2}}-\frac{1}{T_{A1}}\right)} \qquad [-] \qquad (4.13)$$

$$B = \frac{1}{\frac{1}{T_{A2}}-\frac{1}{T_{A1}}}\cdot \ln\frac{L(T_{A2})}{L(T_{A1})} \qquad [K] \qquad (4.14)$$

Vznik poruch představuje náhodný proces, a proto u systémů složených z většího počtu prvků dojde při zkouškách při rozdílných teplotách ke vzniku poruch jiných prvků systému nebo jiným typům poruch. Proto tento přístup představuje jistou míru zjednodušení, kdy systém složený z většího počtu prvků je nahrazen jedním blokem, charakterizovaným jediným parametrem B.



Obr. č. 4.7: Schéma zkoušky, blokový diagram bezporuchovosti systému

V blokovém diagramu bezporuchovosti má elektronický systém prvky uspořádané v sériové soustavě, tzn. při poruše kteréhokoliv prvku vzniká i porucha systému. V teoretickém modelu spolehlivosti se u jednotlivých prvků předpokládá exponenciální rozdělení pravděpodobnosti dob do poruchy, charakterizované intenzitou poruch λ_i, viz obr. č. 4.7.

Zkouška spolehlivosti probíhá při dvou rozdílných zvýšených teplotách, pro dvě skupiny zkoušených výrobků. Zkušební plány mají označení [n_1, U, r_1] při teplotě T_{A1} a [n_2, U, r_2] při teplotě T_{A2}, přičemž u tohoto modelu platí, že $T_{A1} > T_{A2}$.

U obou zkoušených skupin se výrobky po poruše výrobky nenahrazují. Zkouška v obou případech končí po poruše všech výrobků ve skupině, případně časovým omezením zkoušky. V tomto případě se výrobky, u kterých nevznikla porucha, do zkoušky nezahrnují.

Pro určení neznámé hodnoty parametru B Arrheniova modelu se určí kvantitativní parametry spolehlivosti ze zjištěných dob do poruchy t_{A1i} a t_{A2i} při teplotách T_{A1} a T_{A2} jako bodové odhady střední doby do poruchy, vycházející z předpokladu exponenciálního rozdělení, tedy:

$$L(T_{A1}) = \frac{\sum_{i=1}^{r_1} t_{A1i}}{r_1} \quad [\text{h}] \qquad (4.15)$$

$$L(T_{A2}) = \frac{\sum_{i=1}^{r_2} t_{A2i}}{r_2} \quad [\text{h}] \qquad (4.16)$$

Dosazením výsledků do vztahu (4.14) se získá hodnota parametru B, a tedy lze určit hodnotu faktoru zrychlení A_F pro obě skupiny zkoušených výrobků. Při znalosti hodnoty faktoru zrychlení lze hodnoty dob do poruchy získané při zvýšených teplotách ($A1$, $A2$) přepočítat pro provozní podmínky (U), a tedy:

$$t_{U1i} = t_{A1i} \cdot e^{B\left(\frac{1}{T_U} - \frac{1}{T_{A1}}\right)} \quad [\text{h}] \qquad (4.17)$$

$$t_{U2i} = t_{A2i} \cdot e^{B\left(\frac{1}{T_U} - \frac{1}{T_{A2}}\right)} \quad [\text{h}] \qquad (4.18)$$

Kvantitativní ukazatel spolehlivosti elektronického systému pro provozní podmínky se určí jako jednostranný intervalový odhad střední doby do poruchy pro konfidenční úroveň C.

Dolní mez tohoto intervalu T_D se vypočte z dob do poruchy získaných z obou částí zrychlené zkoušky, přepočtených pro provozní podmínky, s využitím chí-kvadrát rozdělení:

$$T_D \geq \frac{2 \cdot \left(\sum_{i=1}^{r_1} t_{U1i} + \sum_{i=1}^{r_2} t_{U2i} \right)}{\chi^2_{2(r_1+r_2+1);C}} \quad [\text{h}] \qquad (4.19)$$

Intervalový odhad intenzity poruch při provozních podmínkách λ_U, který na dané konfidenční úrovni vyjadřuje, že intenzita poruch základního souboru, tj. všech vyrobených výrobků, je rovna nebo menší než tato hodnota, se určí:

$$\lambda_U \leq \frac{1}{T_D} \quad [\text{h}^{-1}] \qquad (4.20)$$

Konkrétní aplikace uvedeného postupu řešení zrychlených zkoušek pro soustavy tvořené elektronickými prvky je uvedena v kapitole č. 7.2.

5 KVALITATIVNÍ ANALÝZA SPOLEHLIVOSTI MODULU UniAVV

Modul UniAVV, vyráběný společností MSV elektronika s.r.o., představuje základní funkční a diagnostickou část systému automatického vedení vlaku (AVV). Vzhledem ke skutečnosti, že systém AVV do značné míry zastupuje některé funkce strojvedoucího hnacího vozidla, je nutné pro realizaci bezpečného provozu železniční dopravy zajistit požadovanou úroveň spolehlivosti tohoto systému, včetně modulu UniAVV.

Pro zajištění bezpečné jízdy vlaku, jehož hnací vozidlo je řízeno v automatizovaném režimu, je nutné identifikovat případná rizika, spojená s činností systému AVV, zejména při selhání požadovaných funkcí. Porucha subsystému či součásti modulu UniAVV, která vyvolá selhání požadované funkce, může zamezit realizaci automatického vedení konkrétního vozidla, rovněž ale může způsobit ohrožení bezpečnosti jízdy daného vlaku, případně ohrozit vlaky nacházející se v jeho blízkosti. Taková porucha může mít katastrofické důsledky a může tedy ovlivnit zdraví a životy desítek osob.

Cílem kvalitativní analýzy spolehlivosti je tedy identifikace poruch funkcí systému AVV, s důrazem na rizikové funkce, jejichž selhání může způsobit ohrožení bezpečnosti železničního provozu. Pro tyto účely je využita analýza způsobů a důsledků poruch (FMEA), jež je vhodným nástrojem pro hodnocení závažnosti rizik.

U identifikovaných kritických funkcí systému AVV je žádoucí, aby nedocházelo k jejich selhání a tím k ohrožení bezpečnosti. Eliminace rizika na nejnižší možnou, společensky přijatelnou úroveň, je pro uvedený systém provedena s využitím principů funkční bezpečnosti, kdy jsou definovány požadavky na dosažení dané úrovně integrity bezpečnosti (SIL). Přiřazení úrovně SIL, nutné pro redukci rizika na přípustnou úroveň, je pro kritické funkce systému AVV provedeno kvalitativní metodou hodnocení rizika.

5.1 Analýza způsobů a důsledků poruch (FMEA)

Pro hodnocení funkcí systému AVV, jejich možného selhání a závažnosti ve vztahu k vyšším úrovním systému, tj. k hnacímu vozidlu jako celku, k vlaku taženému daným hnacím vozidlem, resp. k nejvyšší úrovni, tj. systému železniční dopravy, je použita induktivní metoda FMEA, tedy analýza způsobů a důsledků poruch. Tato metoda zkoumá,

jakým způsobem mohou poruchy celků na nižší úrovni ovlivnit bezporuchovost a bezpečnost vyšších úrovní systémů a hodnotí závažnost těchto selhání [8].

Kvalitativní hodnocení rizika poruch funkcí systému AVV je provedeno s využitím ukazatele RPN (Risk Priority Number), který zahrnuje vliv závažnosti poruchy, její četnosti a možnosti detekce, a je dán vztahem [22]:

$$RPN = ES \cdot CO \cdot CD \quad [-] \tag{5.1}$$

kde: *ES* je závažnost důsledku poruchy,
CO je četnost vzniku poruchy,
CD je odhalitelnost poruchy.

Při analýze rizika daného systému nejsou posuzovány konkrétní technická opatření související s bezpečností, vedoucí ke snížení rizika na přijatelnou úroveň. Při této počáteční analýze jsou uvažovány pouze vnější prostředky ke snížení rizika (mimo systém AVV).

5.1.1 Kritéria provedení analýzy

Analýza FMEA systému automatického vedení vlaku (AVV) je prováděna pro základní funkce realizované modulem UniAVV, zajišťované funkčními moduly CRV (centrální řízení vozidla), RCB (regulace cílového brzdění) a OJV (optimalizace jízdy vlaku). Jsou uvažovány možné způsoby vzniku poruch jednotlivých funkcí a jejich příčiny, avšak bez zahrnutí vlivu konkrétního technického řešení modulu UniAVV (redundance hardware, vlastní diagnostický systém apod.).

Klasifikace závažnosti důsledků poruchy je modifikována pro provoz železničních vozidel (tab. č. 5.1). Poruchy modulu UniAVV mohou mít pro železniční provoz následující závažnost:

- nevýznamná porucha – porucha, která neovlivňuje funkce modulu UniAVV ani provoz vozidel,
- nezávažná porucha – porucha, jejímž důsledkem je nemožnost řízení vozidla s využitím modulu UniAVV, strojvedoucí musí řídit vozidlo ručně.
- závažná porucha – porucha, v jejímž důsledku vzniká významnější zpoždění vlaku,
- kritická porucha – porucha, která způsobí náhlou úplnou ztrátu provozuschopnosti vozidla,

- katastrofická porucha – porucha, která způsobí ohrožení bezpečnosti železničního provozu, v jejímž důsledku může dojít ke zranění nebo usmrcení několika osob, ohrožení životního prostředí apod., např. vlivem vykolejení nebo srážky vozidel apod.

V analýze závažnosti poruch je zvažován vždy jen nejzávažnější důsledek dané poruchy, i když se může jevit jako krajně nepravděpodobný.

Tabulka č. 5.1: Klasifikace závažnosti poruchy (ES)

ES	Typ poruchy	Popis
1-2	nevýznamná	bez dopadu na provoz
3-4	nezávažná	nutnost manuálního řízení vozidla
5-6	závažná	vznik zpoždění vlaku
7-8	kritická	úplná ztráta provozuschopnosti vozidla
9-10	katastrofická	ohrožení bezpečnosti

Četnost vzniku poruchy modulu UniAVV (tab. č. 5.2) je posuzována na základě kvalifikovaného odhadu ve spolupráci s pracovníky vývoje modulu. Při hodnocení četnosti poruch je zohledněno:

- umístění prvku modulu ve vozidle – vyšší četnost poruch je u prvků, které se nacházejí v pojezdu vozidla (vliv vlhkosti, teploty, vibrací apod.), nižší četnost u prvků modulu, které se nacházejí izolovaně ve strojovně,
- počet subsystémů pro přenos a zpracování signálu – četnost poruch vzrůstá s množstvím prvků (procesorové desky, sběrnice, dvoubránové paměti apod.),
- četnost vyžádání funkce – vyšší četnost při nepřetržitém vyžádání funkce, nižší četnost, pokud je funkce s nízkým vyžádáním,
- vliv lidského činitele – poruchy způsobené chybou obsluhy vozidla mají vyšší četnost než poruchy elektronických prvků modulu.

Tabulka č. 5.2: Klasifikace četnosti poruchy (CO)

CO	Četnost poruchy	CO	Četnost poruchy
1	téměř nikdy	6	střední
2	velice slabá	7	mírně zvýšená
3	velice mírná	8	vysoká
4	mírná	9	velmi vysoká
5	nízká	10	téměř jistá

Klasifikace odhalitelnosti poruchy (tab. č. 5.3) vychází z uvedeného předpokladu, že při analýze FMEA není uvažován vlastní diagnostický systém modulu UniAVV. Detekce poruchy je tak možná pouze vnějšími prostředky mimo modul UniAVV, tj. obsluhou vozidla na základě informací signalizovaných na stanovišti strojvedoucího (provozní displeje, mobilní část vlakového zabezpečovače, tlak v hlavním potrubí pneumatické brzdy apod.).

Tabulka č. 5.3: Klasifikace odhalitelnosti poruchy (CD)

CD	Odhalitelnost poruchy	CD	Odhalitelnost poruchy
1	téměř jistá	6	nízká
2	velmi vysoká	7	mírná
3	vysoká	8	velice mírná
4	mírně zvýšená	9	velice slabá
5	střední	10	téměř nemožná

5.1.2 Počáteční analýza FMEA

Počáteční analýza způsobů a důsledků poruch (FMEA) je prováděna v souladu s projektem „Design FMEA“, popsaným v [22]. Pro každou funkci funkčních modulů CRV, resp. RCB a OJV jsou určeny možné způsoby poruchy, jejich důsledek, možné příčiny, je provedeno ohodnocení závažnosti, četnosti výskytu poruchy a odhalitelnosti poruchy pro výpočet hodnoty indexu rizika RPN.

U jednotlivých funkcí modulu UniAVV se předpokládá jejich selhání způsobem ztráty nebo chyby požadované funkce. Ztráta funkce představuje způsob poruchy, kdy požadovaná funkce není dostupná vlivem poruchy hardware zařízení, přerušení přenosu signálu apod. Tato porucha je poměrně snadno zjistitelná vnějšími prostředky (např. není aktivován brzdový systém vozidla před blížícím se místem zastavení atd.). Naproti tomu chyba funkce představuje obtížně detekovatelnou poruchu prostřednictvím vnějších prostředků. Při této poruše modul vykonává činnost, ale výstupní hodnota požadované funkce je nesprávná v dané konkrétní situaci (např. před blížícím se místem zastavení je aktivován brzdový systém vozidla, vlivem chyby funkce je ale brzdný účinek nedostatečný, možnost pozdní detekce poruchy, čímž může dojít k nebezpečné události). Četnost chyby požadované funkce je na základě kvalifikovaného odhadu volena nižší než je četnost ztráty požadované funkce.

Uvedený projekt provádění analýzy FMEA předpokládá určení příčin jednotlivých poruch funkcí. Vzhledem ke skutečnosti, že tato analýza je prováděna jako počáteční, kdy

není k dispozici konkrétní technická specifikace systému, jsou příčiny poruch uváděny pouze na úrovni funkčních celků systému AVV. Jednotlivé příčiny tak představují ztrátu nebo chybu při přenosu signálu v subsystémech vstupů a výstupů, resp. ztrátu nebo chybu signálu při jeho zpracování v bloku logiky modulu UniAVV. Jsou zahrnuty také externí příčiny mimo systém AVV, např. vliv lidského činitele (strojvedoucí, pracovníci údržby), chybně zpracované údaje v palubní mapě tratě apod. Seznam příčin poruch zvažovaných v následné analýze FMEA je uveden v tabulce č. 5.4.

Tabulka č. 5.4: Seznam příčin poruch systému AVV

Označení	Příčina poruchy
EXT_02	Chybné identifikační údaje MIB v palubní mapě trati.
EXT_03	Chybné údaje v palubní mapě trati a palubním jízdním řádu.
INP_01	Ztráta signálu ze snímačů otáček dvojkolí (snímače, vodiče).
INP_02	Ztráta signálu poměrného tahu hl. jízdní páky při přenosu do AVV z VTCU.
INP_03	Porucha snímačů informačních bodů nebo jejich přívodní kabeláže.
INP_04	Nesprávná činnost snímačů informačních bodů (rušení apod.).
INP_05	Ztráta signálu z klávesnice při přenosu do modulu AVV.
INP_06	Ztráta signálu mobilní části vlakového zabezpečovače do AVV.
INP_07	Změna hodnoty signálu ze snímačů otáček dvojkolí (snímače, vodiče).
LOG_01	Ztráta signálu při přenosu a zpracování v bloku logiky (desky, sběrnice).
LOG_02	Změna hodnoty signálu při přenosu a zpracování v bloku logiky (desky, sběrnice).
MAN_01	Chybné zadání průměru dvojkolí pracovníkem údržby.
MAN_02	Chybné zadání délky vlaku strojvedoucím.
MAN_03	Výběr nesprávného čísla vlaku strojvedoucím.
MAN_04	Zadání nesprávné rychlosti strojvedoucím pro vícepovolující návěstní znak.
OUT_01	Ztráta signálu na výstupu z AVV, při přenosu do VTCU (paměť RAM).
OUT_02	Ztráta signálu na výstupu z AVV, při přenosu do brzdiče BSE.
OUT_03	Ztráta signálu na výstupu z AVV, při přenosu vlakovou komunikační sběrnicí NVL.
OUT_04	Změna hodnoty signálu při přenosu do VTCU (paměť RAM).
OUT_05	Změna hodnoty signálu při přenosu vlakovou komunikační sběrnicí NVL ČD.
OUT_06	Změna hodnoty signálu na výstupu z AVV, při přenosu do brzdiče BSE.

Analýza FMEA základních funkcí modulu UniAVV je provedena v tabulce č. 5.5 pro modul CRV a v tabulce č. 5.6 pro moduly RCB a OJV. Vyhodnocení výsledků analýzy je zobrazeno v matici Závažnost x RPN (obr. č. 5.1). Jednotlivé příčiny poruch funkcí se nalézají ve třech oblastech:

- červená – nutnost provést opatření vedoucí ke snížení rizika,
- žlutá – nutnost zvážit provedení opatření vedoucí ke snížení rizika,
- zelená – není nutné provádět opatření ke snížení rizika.

Tabulka č. 5.5: Analýza FMEA – modul CRV

č.	Funkce	Způsob poruchy	Následek	Závažnost	Příčina	Výskyt	Detekce	RPN	Σ RPN
1	Určení rychlosti otáčení dvojkolí, výpočet okamžité rychlosti vozidla.	Ztráta požadované funkce.	Nelze zjistit hodnotu rychlosti vozidla. Nutnost odpojení modulu AVV a manuální řízení vozidla.	3	INP_01	5	2	30	216
					LOG_01	3	2	18	
		Chyba požadované funkce.	Skutečná rychlost je nižší než vypočtená rychlost. Možnost vzniku zpoždění.	5	LOG_02	1	3	15	
					MAN_01	2	3	30	
					INP_07	1	3	15	
		Chyba požadované funkce.	Skutečná rychlost je vyšší než vypočtená rychlost. Nebezpečí vykolejení.	9	LOG_02	1	3	27	
					MAN_01	2	3	54	
					INP_07	1	3	27	
2	Zajištění protismykové a protiskluzové ochrany (jednotlivých dvojkolí, synchronní).	Ztráta požadované funkce.	Neprovozuschopná protismyková a protiskluzová ochrana. Možnost vzniku zpoždění.	5	INP_01	5	2	50	306
					LOG_01	3	8	120	
					OUT_01	2	2	20	
					OUT_02	2	2	20	
		Chyba požadované funkce.	Změna hodnoty signálu PT+, PT- pro VTCU, resp. brzdič BSE.	6	LOG_02	1	8	48	
					OUT_04	1	8	48	
3	Regulace kladného poměrného tahu na základě požadavku (hl. jízdní páka, ARR).	Ztráta požadované funkce.	Nelze zadat požadovaný poměrný tah. Nutnost odpojení modulu AVV a manuální řízení vozidla.	3	INP_02	2	2	12	92
					LOG_01	3	2	18	
					OUT_01	2	2	12	
		Chyba požadované funkce.	Skutečná hodnota PT+ nižší než požadovaná. Možnost vzniku zpoždění.	5	LOG_02	1	5	25	
					OUT_04	1	5	25	
4	Regulace záporného poměrného tahu na základě požadavku (hl. jízdní páka, ARR).	Ztráta požadované funkce.	Není zajištěn požadovaný brzdný účinek. Nebezpečí vykolejení, projetí návěsti Stůj.	10	INP_02	2	2	40	330
					LOG_01	3	2	60	
					OUT_01	2	2	40	
					OUT_02	2	2	40	
		Chyba požadované funkce.	Nedostatečná hodnota PT-, nebezpečí vykolejení, projetí návěsti Stůj.	10	LOG_02	1	5	50	
					OUT_04	1	5	50	
					OUT_06	1	5	50	
5	Zajištění součinnosti pneumatické a elektrodynamické brzdy (vystřídací brzda).	Ztráta požadované funkce.	Nedostatečný brzdný účinek. Nebezpečí vykolejení, projetí návěsti Stůj.	10	INP_01	5	2	100	240
					LOG_01	3	2	60	
		Chyba požadované funkce.	Nedostatečný brzdný účinek. Nebezpečí vykolejení, projetí návěsti	10	LOG_02	1	5	50	
					INP_07	1	3	30	

Tabulka č. 5.5: Analýza FMEA – modul CRV, pokračování

č.	Funkce	Způsob poruchy	Následek	Závažnost	Příčina	Výskyt	Detekce	RPN	Σ RPN
6	Respektování délky vlaku ke konci pomalé jízdy.	Ztráta požadované funkce.	Nečinná funkce, nutný zásah strojvedoucího.	4	LOG_01	3	2	24	159
		Chyba požadované funkce.	Zrychlování vlaku v úseku pomalé jízdy. Nebezpečí vykolejení.	9	MAN_02	3	5	135	
7	Vyhodnocení signálů ze snímačů MIB.	Ztráta požadované funkce.	Nelze přesně identifikovat polohu vozidla. Aktivace brzdění vlaku, vznik	6	INP_03	5	2	60	156
					LOG_01	3	2	36	
		Chyba požadované funkce.	Nesprávná identifikace polohy vozidla. Nebezpečí projetí návěsti Stůj,	10	LOG_02	1	3	30	
					INP_04	1	3	30	
8	Zajištění mnohočlenného řízení vozidel v režimu AVV (přenos signálu PT).	Ztráta požadované funkce.	Není zajištěn přenos signálu PT do řízených vozidel. Nebezpečí	10	OUT_03	2	5	100	390
					LOG_01	3	5	150	
		Chyba požadované funkce.	Nesprávná hodnota signálu PT pro řízená vozidla. Nebezpečí vykolejení,	10	LOG_02	1	7	70	
					OUT_05	1	7	70	
9	Zajištění komunikace se strojvedoucím (klávesnice).	Ztráta požadované funkce.	Nelze zadat parametry pro ARR, RCB, OJV. Nutnost manuálního řízení	5	INP_05	2	2	20	20
					LOG_01	3	2	30	
10	Signalizace provozních informací ze systému AVV strojvedoucímu (displej).	Ztráta požadované funkce.	Strojvedoucí není informován o činnosti (nečinnosti) AVV. Odpojení	8	LOG_01	3	2	48	220
					OUT_01	2	2	32	
		Chyba požadované funkce.	Strojvedoucí je nesprávně informován o činnosti (nečinnosti) AVV. Nebezpečí vykolejení, projetí návěsti Stůj.	10	LOG_02	1	7	70	
					OUT_04	1	7	70	
11	Zajištění kontroly správných kombinací signálů, které umožňují jízdu vlaku.	Ztráta požadované funkce.	Nebezpečí poškození významných konstrukčních celků vozidla.	7	LOG_01	3	3	63	84
		Chyba požadované funkce.	Nebezpečí poškození významných konstrukčních celků vozidla.	7	LOG_02	1	3	21	

Tabulka č. 5.6: Analýza FMEA – moduly RCB a OJV

č.	Funkce	Způsob poruchy	Následek	Závažnost	Příčina	Výskyt	Detekce	RPN	Σ RPN
1	Idenfitikace polohy vozidla na trati.	Chyba požadované funkce.	Nelze přesně identifikovat polohu vozidla. Nebezpečí vykolejení, projetí návěsti Stůj.	10	EXT_02	1	2	20	120
					MAN_01	2	2	40	
					MAN_03	3	2	60	
2	Načítání dat z palubní mapy tratě a palubního jízdního řádu.	Ztráta požadované funkce.	Nejsou k dispozi potřebná data. Nutnost aktivace režimu ARR nebo MAN.	3	LOG_01	2	2	12	162
		Chyba požadované funkce.	Načítání nesprávných dat. Nebezpečí vykolejení, projetí návěsti Stůj.	10	EXT_03	1	4	40	
					MAN_03	3	2	60	
					LOG_02	1	5	50	
3	Realizace cílového brzdění (výpočet požadované rychlosti pro ARR v závislosti na poloze).	Ztráta požadované funkce.	Není realizováno cílové brzdění. Nebezpečí vykolejení nebo projetí návěsti Stůj.	10	LOG_01	2	3	60	130
		Chyba požadované funkce.	Chybná hodnota požadované rychlosti. Nebezpečí vykolejení nebo projetí návěsti Stůj.	10	LOG_02	1	7	70	
4	Realizace energeticky optimální jízdní strategie.	Ztráta požadované funkce.	Není realizována energeticky optimální jízda.	3	LOG_01	2	7	42	77
		Chyba požadované funkce.	Chybně realizovaná energeticky optimální jízda. Možnost vzniku zpoždění.	5	LOG_02	1	7	35	
5	Vyhodnocování kódu mobilní části vlakového zabezpečovače.	Ztráta požadované funkce.	Vozidlo realizuje cílové brzdění podle nejzávažnějšího možného návěstního	6	INP_06	2	2	24	340
					LOG_01	3	2	36	
		Chyba požadované funkce.	Cílové brzdění k nesprávné návěsti oproti VZ. Nebezpečí vykolejení,	10	LOG_02	1	3	30	
					MAN_04	5	5	250	

Obr. č. 5.1: Matice RPN x Závažnost

Risk Priority Number (RPN)		1, 2 nevýznamná	3, 4 nezávažná	5, 6 závažná	7, 8 kritická	9, 10 katastrofická
	250					5_MAN_04;
	225					
	200					
	175					
	150					6_MAN_02; 8_LOG_01;
	125			2_LOG_01;		
	100					5_INP_01; 8_OUT_03; 8_LOG_02; 8_OUT_05;
	75			7_INP_03;	11_LOG_01;	1_MAN_01; 4_LOG_01; 5_LOG_01; 10_LOG_02; 10_OUT_04; 1_MAN_03; 2_MAN_03; 3_LOG_01; 3_LOG_02;
	50		1_INP_01; 4_LOG_01;	1_MAN_01; 2_INP_01; 2_LOG_02; 2_OUT_04; 7_LOG_01; 9_LOG_01; 4_LOG_02; 5_LOG_01;	10_LOG_01; 10_OUT_01;	1_LOG_02; 1_INP_07; 4_INP_02; 4_OUT_01; 4_OUT_02; 4_LOG_02; 4_OUT_04; 4_OUT_06; 5_INP_07; 5_LOG_02; 7_LOG_02; 7_INP_04; 1_MAN_01; 2_EXT_03; 2_LOG_02; 5_LOG_02;
	25		1_LOG_01; 3_INP_02; 3_LOG_01; 3_OUT_01; 6_LOG_01; 2_LOG_01;	1_LOG_02; 1_INP_07; 2_OUT_01; 2_OUT_02; 3_LOG_02; 3_OUT_04; 9_INP_05; 5_INP_06;	11_LOG_02;	1_EXT_02;

Legenda:

CRV
RCB+OJV

Č.Funkce_Ozn.příčiny

Bez opatření
Možné opatření
Nutné opatření

Z výsledků analýzy (matice závažnost x RPN) vyplývá, že opatření vedoucí ke snížení rizika je nutné provést pro funkce, jejichž poruchy mohou ohrozit bezpečnost provozu (kategorie katastrofická porucha, červená oblast matice). Seznam těchto funkcí a jejich příčin modulu UniAVV je uveden v tabulce č. 5.7.

Tabulka č. 5.7: Funkce modulu UniAVV – nutnost opatření ke snížení rizika

Označení	Funkce	Příčina poruchy
1_LOG_02	Určení rychlosti vozidla	Blok logiky (chyba funkce)
1_MAN_01	Určení rychlosti vozidla	Chybné zadání průměru kola
1_INP_07	Určení rychlosti vozidla	Chybný signál snímače otáček
4_INP_02	Regulace záporného poměrného tahu	Ztráta signálu z hlavní jízdní páky (RAM)
4_LOG_01	Regulace záporného poměrného tahu	Blok logiky (ztráta funkce)
4_LOG_02	Regulace záporného poměrného tahu	Blok logiky (chyba funkce)
4_OUT_01	Regulace záporného poměrného tahu	Ztráta signálu do VTCU (RAM)
4_OUT_02	Regulace záporného poměrného tahu	Ztráta signálu do brzdiče BSE
4_OUT_04	Regulace záporného poměrného tahu	Změna signálu do VTCU (RAM)
4_OUT_06	Regulace záporného poměrného tahu	Změna signálu do brzdiče BSE
5_INP_01	Součinnost brzd (vystřídání brzd)	Ztráta signálu snímače otáček
5_INP_07	Součinnost brzd (vystřídání brzd)	Chybný signál snímače otáček
5_LOG_01	Součinnost brzd (vystřídání brzd)	Blok logiky (ztráta funkce)
5_LOG_02	Součinnost brzd (vystřídání brzd)	Blok logiky (chyba funkce)
6_MAN_02	Respektování délky vlaku (pomalá jízda)	Chybné zadání délky vlaku
7_INP_04	Vyhodnocení signálů snímačů MIB	Změna signálu z MIB
7_LOG_02	Vyhodnocení signálů snímačů MIB	Blok logiky (chyba funkce)
8_LOG_01	Mnohočlenné řízení vozidel	Blok logiky (ztráta funkce)
8_LOG_02	Mnohočlenné řízení vozidel	Blok logiky (chyba funkce)
8_OUT_03	Mnohočlenné řízení vozidel	Změna signálu do sběrnice NVL ČD
8_OUT_05	Mnohočlenné řízení vozidel	Změna signálu do sběrnice NVL ČD
10_LOG_02	Signalizace strojvedoucímu na displeji	Blok logiky (chyba funkce)
10_OUT_04	Signalizace strojvedoucímu na displeji	Změna signálu do VTCU (RAM)
1_EXT_02	Identifikace vozidla na trati	Chybné údaje MIB v palubní mapě trati
1_MAN_01	Identifikace vozidla na trati	Chybné zadání průměru kola
1_MAN_03	Identifikace vozidla na trati	Chybné zadání čísla vlaku
2_EXT_03	Načítání dat z mapy trati, jízdního řádu	Chybné údaje v palubní mapě trati
2_LOG_02	Načítání dat z mapy trati, jízdního řádu	Blok logiky (chyba funkce)
2_MAN_03	Načítání dat z mapy trati, jízdního řádu	Chybné zadání trati, vlaku
3_LOG_01	Realizace cílového brzdění	Blok logiky (ztráta funkce)
3_LOG_02	Realizace cílového brzdění	Blok logiky (chyba funkce)
5_LOG_02	Vyhodnocení kódu vlakového zabezp.	Blok logiky (chyba funkce)
5_MAN_04	Vyhodnocení kódu vlakového zabezp.	Chybné zadání rychlosti pro návěst

Z výsledků výše uvedené analýzy vyplývá, že významné riziko spojené s ohrožením bezpečnosti železničního provozu vyvolává selhání funkcí modulu UniAVV, jež jsou spojeny s činností brzdového systému vozidla, resp. vlaku (funkce regulace brzdného účinku, funkce

součinnosti EDB a pneumatické brzdy). Velké riziko způsobuje rovněž porucha funkce identifikace polohy vozidla na trati (nesprávný přenos informací z traťových magnetických bodů, případně nesprávné údaje v palubní mapě trati), nebo porucha přenosu informací z mobilní části vlakového zabezpečovače.

Selhání brzdového systému hnacího vozidla, resp. vlaku, které je způsobeno poruchou funkce modulu UniAVV, může v krajním případě zapříčinit katastrofální důsledky s vlivem na lidské zdraví a životy, nebo životní prostředí. Nebezpečná situace může nastat v případě, kdy se vlak blíží k návěstidlu s návěstí pro snížení rychlosti a brzdný účinek vlaku je nedostatečný. V případě, že na toto selhání strojvedoucí zareaguje pozdě, nebo nereaguje vůbec, hrozí za návěstidlem, pokud se nachází v místě zhlaví železniční stanice, vykolejení vlaku. Další nebezpečná situace může vzniknout při jízdě vlaku k návěstidlu s návěstí „Stůj“. V případě nedostatečného brzdného účinku vlaku hrozí nebezpečí přejetí vlaku za toto návěstidlo, což může ohrozit vlaky a vozidla nacházející se v tomto úseku a v krajním případě může dojít ke srážce vozidel.

Další velmi nebezpečné situace může vyvolat nesprávná identifikace polohy vozidla na trati na základě přenosu informace z magnetického informačního bodu (MIB) nebo chybných údajů v palubní mapě trati. Tyto situace jsou obzvlášť nebezpečné na vjezdových zhlavích železničních stanic, kdy jízda vlaku může pokračovat po různých kolejích. Nesprávnou identifikací koleje, po které vlak jede, a její záměna za jinou může způsobit v krajním případě vykolejení vlaku nebo srážku s jiným vozidlem.

Nezanedbatelné riziko pro železniční provoz, vyplývající z činnosti modulu UniAVV, je spojeno s vlivem lidského činitele. Významnost tohoto rizika stupňuje skutečnost, že pokud osoba spojená se správnou činností dané funkce způsobí chybu, nelze dalšími vnějšími prostředky tuto skutečnost odhalit. Typický příklad představuje u modulu UniAVV zadávání požadované rychlosti pro vícestavové znaky přenášené vlakovým zabezpečovačem. Při chybném zadání požadované rychlosti může nastat situace, kdy vlak pojede rychlostí vyšší, než je rychlost dovolená, čímž může dojít k jeho vykolejení.

Z výše uvedené analýzy způsobů a důsledků poruch pro modul UniAVV vyplývá, že při provozu tohoto zařízení mohou nastat nebezpečné situace, jež mohou ojediněle vyústit v katastrofické důsledky. Je krajně nežádoucí, aby tyto situace při režimu automatického vedení vlaku nastaly, a proto je nezbytné nalézt opatření pro funkce modulu UniAVV, které nutně vyžadují snížení rizika.

5.2 Stanovení požadavků na redukci rizika

Snížení rizika na přípustnou úroveň je u modulu UniAVV provedeno v souladu s normou ČSN EN 61508, jež definuje požadavky na funkční bezpečnost E/E/PE systémů souvisejících s bezpečností. Opatření k eliminaci rizika vycházející z principů funkční bezpečnosti jsou založena na dosažení velmi nízké pravděpodobnosti vzniku nebezpečné události a jejím předcházení prováděním vysoce účinných diagnostických testů. Úroveň dosažené funkční bezpečnosti je u těchto systémů charakterizována hodnotou úrovně integrity bezpečnosti (SIL).

Požadavky na potřebnou úroveň integrity bezpečnosti jsou u modulu UniAVV určeny pro funkce, jejichž selhání může způsobit ohrožení bezpečnosti železniční dopravy. Přiřazení požadavků na SIL je provedeno kvalitativním hodnocením rizika vyplývajícího z činnosti modulu. Pro analýzu je využita metoda diagramu rizika, která je popsána v kapitole č. 3.2.2.

5.2.1 Určení integrity bezpečnosti modulu UniAVV

Pro určení úrovní integrity bezpečnosti (SIL) modulu UniAVV je využita metoda diagramu rizika, která je založena na hodnocení následků nebezpečné události, pravděpodobnosti vzniku této události a posouzení, za jakých možností je možné se nebezpečné události vyhnout. Podle stanovených kategorií těchto ukazatelů hodnocení rizika jsou pro analýzu vybrány pouze ty funkce modulu UniAVV, jejichž následkem může být zranění, zranění s trvalými následky, smrt jedné, několika nebo velkého počtu osob. Tomu v analýze FMEA odpovídají funkce, vlivem jejichž selhání může dojít k ohrožení bezpečnosti provozu (katastrofická porucha).

Vstupními údaji pro použití diagramu rizika jsou výstupy analýzy FMEA modulu UniAVV. Jednotlivé kategorie parametrů rizika v diagramu rizika kvalitativně odpovídají parametrům hodnocení významnosti poruch (RPN – Risk Priority Number) v analýze FMEA.

Vyhodnocení úrovně integrity bezpečnosti je provedeno pro každou příčinu poruchy sledovaných funkcí modulu UniAVV. Výsledná požadovaná úroveň integrity bezpečnosti (SIL) je u jednotlivých subsystémů modulu UniAVV určena podle nejvíce rizikové příčiny poruchy funkce. Se zvyšujícím se rizikem nebezpečné události a z toho vyplývajícími důsledky se zvětšují požadavky na opatření ke snížení tohoto rizika. To je charakterizováno vyšší požadovanou úrovní integrity bezpečnosti (SIL).

Pro funkce modulu UniAVV je hodnocení rizika provedeno klasifikací jeho jednotlivých parametrů podle stanovených stupnic a následným trasováním v diagramu rizika, z čehož vyplyne požadavek na potřebnou úroveň integrity bezpečnosti. Příklad klasifikace jednotlivých parametrů rizika pro vybranou funkci modulu UniAVV je uveden v tabulce č. 5.8. V diagramu na obr. č. 5.2 je pro tuto funkci zobrazen diagram rizika se postupem stanovení požadované úrovně SIL.

Tabulka č. 5.8: Příklad klasifikace parametrů rizika funkce modulu UniAVV

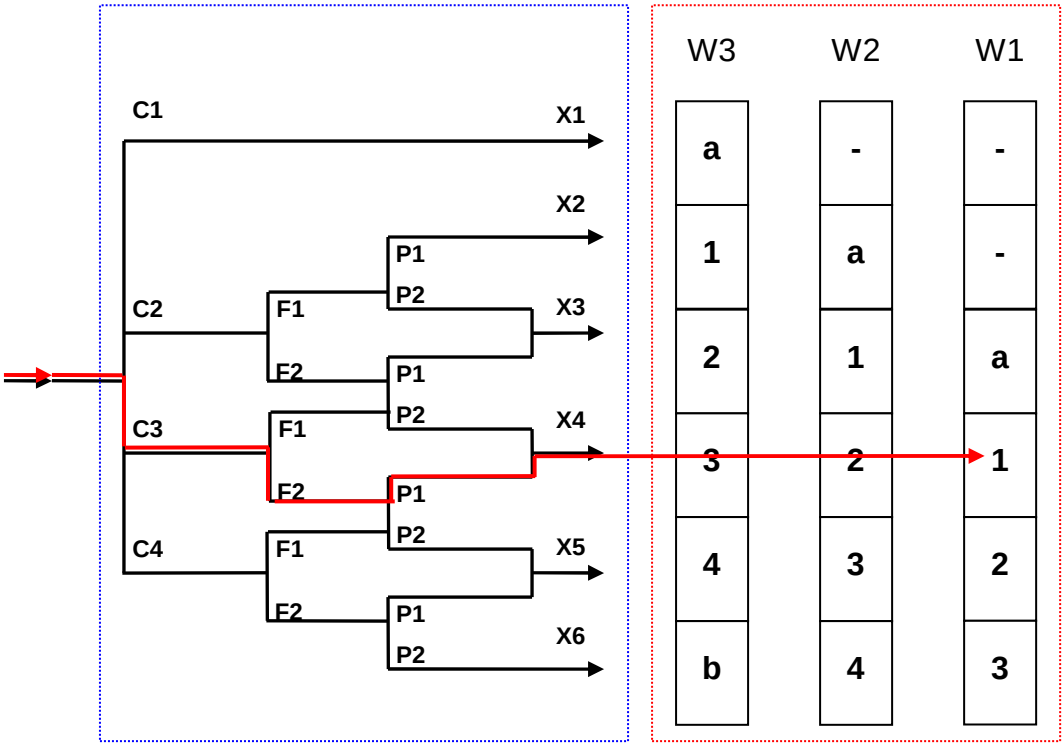
Funkce:	4_CRV	Regulace záporného poměrného tahu na základě požadavku (hl. jízdní páka, modul ARR).	
Příčina poruchy:	LOG_01	Ztráta signálu při přenosu a zpracování v bloku logiky.	
Diagram rizika – parametry rizika			
Parametr	**Kategorie**	**Popis**	**Zdůvodnění**
Následek (C)	C3	smrt několika osob	Porucha může v krajním případě způsobit vykolejení vozidla (zranění osob – C2) nebo projetí návěsti Stůj, nebezpečí srážky vozidel (smrt několika osob – C3). Volí se závažnější následek.
Režim vyžádání (F)	F2	častá až trvalá doba funkce	Funkce regulace záporného poměrného tahu je trvalá funkce modulu UniAVV.
Možnost vyhnutí nebezpečné události (P)	P1	možnost vyhnutí za určitých podmínek	Není-li funkce regulace záporného poměrného tahu k dispozici (vlak nebrzdí), strojvedoucímu je tato situace signalizována (tlak v hlavním potrubí), může situaci zabránit (použití rychlobrzdy) a má k tomu dostatečný čas (účinek rychlobrzdy je vyšší než při provozním brzdění).
Pravděpodobnost výskytu (W)	W1	velmi malá	Velmi malá pravděpodobnost z důvodu využití elektronických systémů.

Z průběhu trasování v diagramu rizika pro uvedený příklad na obrázku č. 5.2 vyplývá, že funkce regulace záporného poměrného tahu (tedy regulace brzdného účinku vozidla), jejíž selhání je způsobeno ztrátou signálu v subsystému bloku logiky, musí dosahovat úroveň integrity bezpečnosti SIL1.

Přehled přiřazení kategorií parametrů rizika a úrovní integrity bezpečnosti ke všem funkcím modulu UniAVV ovlivňujícím bezpečnost je uveden v tabulce č. 5.9. S využitím stanovených hodnot SIL posuzovaných funkcí jsou následně stanoveny požadavky funkční bezpečnosti pro jednotlivé subsystémy modulu UniAVV a také další subsystémy AVV, které přímo souvisejí s činností modulu (viz obr. č. 5.3).

Diagram rizika

Funkce: 4_CRV Regulace záporného poměrného tahu na základě požadavku (hl. jízdní páka, modul ARR).
Příčina poruchy: LOG_01 Ztráta signálu při přenosu a zpracování v bloku logiky.



- = žádné bezpečnostní požadavky
a = žádné speciální bezpečnostní požadavky
1, 2, 3, 4 = SIL 1, SIL 2, SIL 3, SIL 4
b = jediný systém související s bezpečností není dostatečný

Klasifikace ukazatelů rizika

Následek nebezpečné události	C1	menší zranění
	C2	zranění více osob s trvalými následky, smrt jedné osoby
	C3	smrt několika osob
	C4	smrt velkého počtu osob
Režim vyžádání funkce	F1	vzácná a častější doba funkce
	F2	častá až trvalá doba funkce
Možnost se vyhnout nebezpečné události	P1	možné za určitých podmínek
	P2	téměř nemožné
Pravděpodobnost nežádoucího výskytu	W1	velmi malá
	W2	malá
	W3	poměrně vysoká

Obr. č. 5.2: Příklad přiřazení úrovně integrity bezpečnosti (SIL)

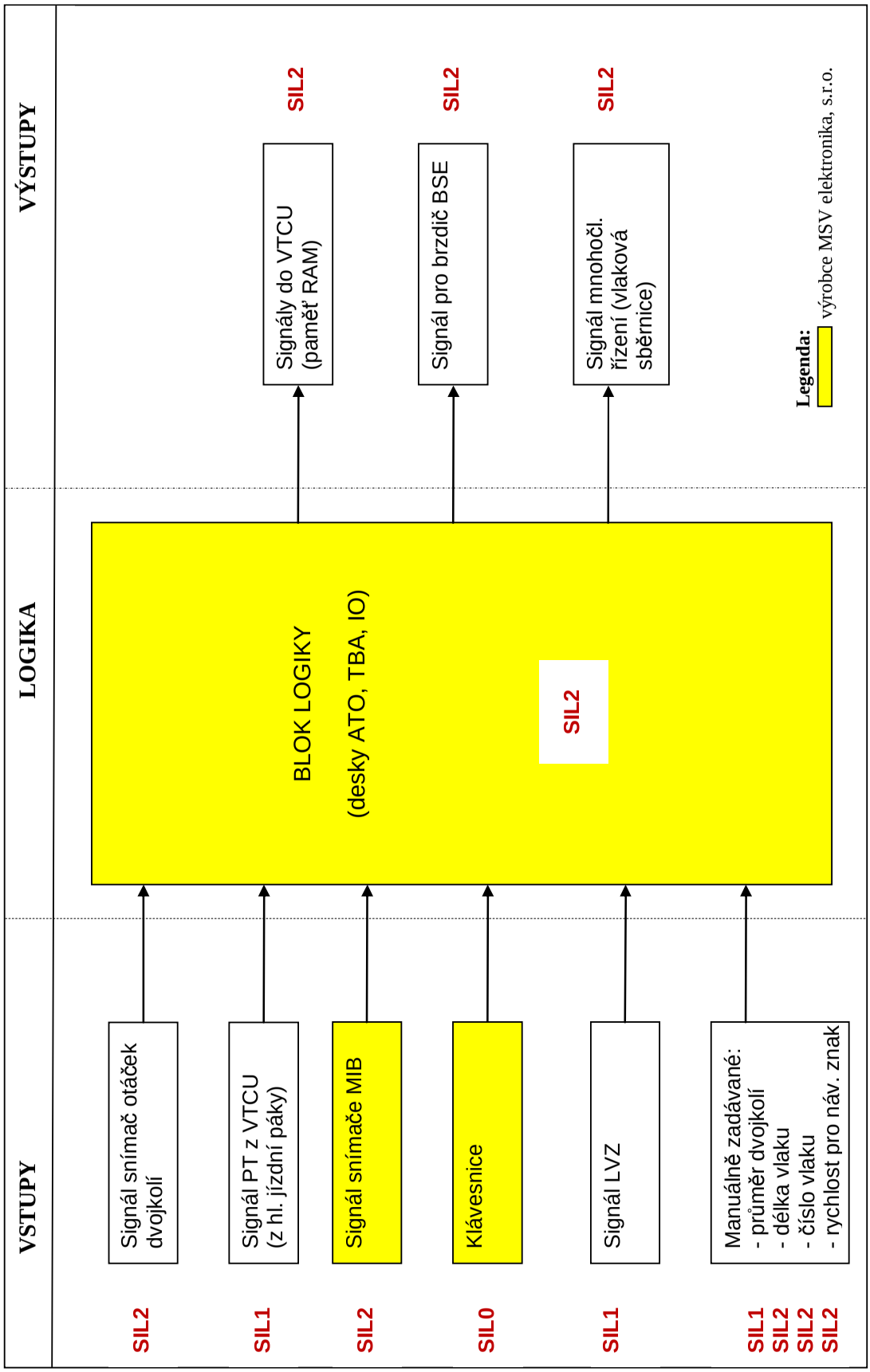
Tabulka č. 5.9: Přiřazení parametrů rizika a úrovní integrity bezpečnosti (SIL)

Označení	Následek	Vyžádání funkce	Možnost vyhnutí	P-ost výskytu	SIL	Funkce	Příčina poruchy
1_LOG_02	C2	F2	P1	W1	-	Určení rychlosti vozidla	Blok logiky (chyba funkce)
1_MAN_01	C2	F2	P1	W1	-	Určení rychlosti vozidla	Chybné zadání průměru kola
1_INP_07	C2	F2	P1	W1	-	Určení rychlosti vozidla	Chybný signál snímače otáček
4_INP_02	C3	F2	P1	W1	SIL1	Regulace záporného poměrného tahu	Ztráta signálu z hlavní jízdní páky (RAM)
4_LOG_01	C3	F2	P1	W1	SIL1	Regulace záporného poměrného tahu	Blok logiky (ztráta funkce)
4_LOG_02	C3	F2	P2	W1	SIL2	Regulace záporného poměrného tahu	Blok logiky (chyba funkce)
4_OUT_01	C3	F2	P1	W1	SIL1	Regulace záporného poměrného tahu	Ztráta signálu do VTCU (RAM)
4_OUT_02	C3	F2	P1	W1	SIL1	Regulace záporného poměrného tahu	Ztráta signálu do brzdiče BSE
4_OUT_04	C3	F2	P2	W1	SIL2	Regulace záporného poměrného tahu	Změna signálu do VTCU (RAM)
4_OUT_06	C3	F2	P2	W1	SIL2	Regulace záporného poměrného tahu	Změna signálu do brzdiče BSE
5_INP_01	C3	F2	P1	W2	SIL2	Součinnost brzd (vystřídání brzd)	Ztráta signálu snímače otáček
5_INP_07	C3	F2	P1	W1	SIL1	Součinnost brzd (vystřídání brzd)	Chybný signál snímače otáček
5_LOG_01	C3	F2	P1	W1	SIL1	Součinnost brzd (vystřídání brzd)	Blok logiky (ztráta funkce)
5_LOG_02	C3	F2	P2	W1	SIL2	Součinnost brzd (vystřídání brzd)	Blok logiky (chyba funkce)
6_MAN_02	C2	F2	P2	W2	SIL2	Respektování délky vlaku (pomalá jízda)	Chybné zadání délky vlaku
7_INP_04	C3	F2	P1	W1	SIL1	Vyhodnocení signálů snímačů MIB	Změna signálu z MIB
7_LOG_02	C3	F2	P1	W1	SIL1	Vyhodnocení signálů snímačů MIB	Blok logiky (chyba funkce)
8_LOG_01	C3	F2	P2	W1	SIL2	Mnohočlenné řízení vozidel	Blok logiky (ztráta funkce)
8_LOG_02	C3	F2	P2	W1	SIL2	Mnohočlenné řízení vozidel	Blok logiky (chyba funkce)
8_OUT_03	C3	F2	P2	W1	SIL2	Mnohočlenné řízení vozidel	Změna signálu do sběrnice NVL ČD
8_OUT_05	C3	F2	P2	W1	SIL2	Mnohočlenné řízení vozidel	Změna signálu do sběrnice NVL ČD
10_LOG_02	C3	F2	P2	W1	SIL2	Signalizace strojvedoucímu na displeji	Blok logiky (chyba funkce)
10_OUT_04	C3	F2	P2	W1	SIL2	Signalizace strojvedoucímu na displeji	Změna signálu do VTCU (RAM)
1_EXT_02	C3	F2	P1	W1	SIL1	Identifikace vozidla na trati	Chybné údaje MIB v palubní mapě trati
1_MAN_01	C3	F2	P1	W1	SIL1	Identifikace vozidla na trati	Chybné zadání průměru kola
1_MAN_03	C3	F2	P1	W2	SIL2	Identifikace vozidla na trati	Chybné zadání čísla vlaku
2_EXT_03	C3	F2	P1	W1	SIL1	Načítání dat z mapy trati, jízdního řádu	Chybné údaje v palubní mapě trati
2_LOG_02	C3	F2	P1	W1	SIL1	Načítání dat z mapy trati, jízdního řádu	Blok logiky (chyba funkce)
2_MAN_03	C3	F2	P1	W2	SIL2	Načítání dat z mapy trati, jízdního řádu	Chybné zadání trati, vlaku
3_LOG_01	C3	F2	P1	W1	SIL1	Realizace cílového brzdění	Blok logiky (ztráta funkce)
3_LOG_02	C3	F2	P2	W1	SIL2	Realizace cílového brzdění	Blok logiky (chyba funkce)
5_LOG_02	C3	F2	P1	W1	SIL1	Vyhodnocení kódu vlakového zabezp.	Blok logiky (chyba funkce)
5_MAN_04	C2	F2	P2	W2	SIL2	Vyhodnocení kódu vlakového zabezp.	Chybné zadání rychlosti pro návěst

Legenda:

CRV
RCB+OJV

Č.Funkce_Ozn.příčiny



Obr. č. 5.3: Přiřazení požadavků SIL subsystémům AVV

Výrobci jednotlivých subsystémů systému automatického vedení vlaku (AVV) přebírají odpovědnost za splnění požadavků funkční bezpečnosti, specifikovaných stanovenou úrovní integrity bezpečnosti (SIL), potřebnou pro snížení rizika na přípustnou úroveň. Výrobce modulu UniAVV, společnost MSV elektronika s.r.o., musí pro splnění požadavků funkční bezpečnosti hardware a software tohoto výrobku prokázat dosažení úrovně integrity bezpečnosti SIL2 (pro subsystém bloku logiky a subsystém přenosu signálu snímače MIB).

5.2.2 Omezení architektury hardware

Z hlediska posuzování ukazatelů funkční bezpečnosti hardware, kterým se zabývá tato práce, je podstatná také problematika uspořádání (omezení) architektury hardware jednotlivých subsystémů modulu UniAVV. V závislosti na uspořádání architektury hardware jsou definovány požadované hodnoty parametrů, které musí posuzované subsystémy dosáhnout, aby splnily stanovenou úroveň integrity bezpečnosti (SIL). Pro hodnocení funkční bezpečnosti hardware jsou těmito parametry diagnostické pokrytí (DC) a cílová míra poruch (PFH), které charakterizují subsystémy související s bezpečností z hlediska kvality provádění diagnostických testů, resp. pravděpodobnosti vzniku nebezpečné události.

Na základě požadavků na úroveň integrity bezpečnosti (SIL) pro subsystémy AVV je navrženo omezení architektury hardware systému pro dva základní principy řešení:

- subsystémy bez redundance (bez zálohování) – představují uspořádání architektury hardware s označením 1oo1 (jednokanálová architektura), kdy při jakékoliv nebezpečné poruše nemůže subsystém vykonávat požadovanou funkci;
- subsystémy s redundancí (se zálohováním) – v tomto případě je uvažována minimální varianta zálohování, kdy architektura hardware má uspořádání s označením 1oo2 (dvoukanálová architektura) a požadovanou funkci může vykonávat libovolný z obou kanálů (odolnost proti poruchám hardware $N = 1$).

Pro jednotlivé kanály subsystémů AVV jsou uvedeny požadované hodnoty základních ukazatelů funkční bezpečnosti hardware, tj. diagnostického pokrytí (DC) a cílové míry poruch (PFH), vyplývající z přiřazené úrovně integrity bezpečnosti, které musí být pro uvedené řešení dodrženy. Splněním požadavků funkční bezpečnosti je pak zajištěno, že pro posuzovaný systém AVV je provedena dostatečná eliminace rizika, vyplývající z jeho činnosti a selhání, čímž se v maximální míře zamezí vzniku nebezpečných událostí, které

mohou ovlivnit bezpečnost železniční dopravy. Požadavky na parametry funkční bezpečnosti pro dvě uvažovaná řešení systému jsou uvedeny v tabulkách č. 5.10 a 5.11.

Tabulka č. 5.10: Omezení architektury modulu UniAVV, systém bez zálohování

Subsystém	Požadavky - subsystém		Požadavky - 1 kanál		
	Architektura	SIL_{sub}	$SIL_{kanál}$	Diagnostické pokrytí [%]	THR [-]
Snímač otáček dvojkolí	1oo1	SIL2	SIL2	90 ÷ 99	$10^{-7} \div 10^{-6}$
Signál PT z VTCU	1oo1	SIL1	SIL1	60 ÷ 90	$10^{-6} \div 10^{-5}$
Snímač MIB	1oo1	SIL2	SIL2	90 ÷ 99	$10^{-7} \div 10^{-6}$
Signál LVZ	1oo1	SIL1	SIL1	60 ÷ 90	$10^{-6} \div 10^{-5}$
Blok logiky	1oo1	SIL2	SIL2	90 ÷ 99	$10^{-7} \div 10^{-6}$
Signál pro VTCU (RAM)	1oo1	SIL2	SIL2	90 ÷ 99	$10^{-7} \div 10^{-6}$
Signál pro brzdič BSE	1oo1	SIL2	SIL2	90 ÷ 99	$10^{-7} \div 10^{-6}$
Signál pro sběrnici NVL ČD	1oo1	SIL2	SIL2	90 ÷ 99	$10^{-7} \div 10^{-6}$

Tabulka č. 5.11: Omezení architektury modulu UniAVV, systém se zálohováním

Subsystém	Požadavky - subsystém		Požadavky - 1 kanál		
	Architektura	SIL_{sub}	$SIL_{kanál}$	Diagnostické pokrytí [%]	Cílová míra poruch [-]
Snímač otáček dvojkolí	1oo2	SIL2	SIL1	60 ÷ 90	$10^{-6} \div 10^{-5}$
Signál PT z VTCU (RAM)	1oo1	SIL1	SIL1	60 ÷ 90	$10^{-6} \div 10^{-5}$
Snímač MIB	1oo2	SIL2	SIL1	60 ÷ 90	$10^{-6} \div 10^{-5}$
Signál LVZ	1oo1	SIL1	SIL1	60 ÷ 90	$10^{-6} \div 10^{-5}$
Blok logiky	1oo2	SIL2	SIL1	60 ÷ 90	$10^{-6} \div 10^{-5}$
Signál pro VTCU (RAM)	1oo2	SIL2	SIL1	60 ÷ 90	$10^{-6} \div 10^{-5}$
Signál pro brzdič BSE	1oo2	SIL2	SIL1	60 ÷ 90	$10^{-6} \div 10^{-5}$
Signál pro sběrnici NVL ČD	1oo2	SIL2	SIL1	60 ÷ 90	$10^{-6} \div 10^{-5}$

Z přiřazení požadavků pro ukazatele funkční bezpečnosti v souvislosti s uspořádáním architektury hardware jednotlivých subsystémů AVV vyplývá, že při použití redundantního paralelního uspořádání kanálů subsystémů lze dosáhnout vyšší úrovně SIL, i když jednotlivé kanály splňují požadavky pouze pro nižší úroveň funkční bezpečnosti.

5.3 Hodnocení výsledků kvalitativní analýzy spolehlivosti

Stanovením požadavků na úroveň integrity bezpečnosti (SIL) na základě provedené kvalitativní analýzy spolehlivosti modulu UniAVV jsou jasně definována opatření vedoucí ke snížení jeho rizika na přijatelnou úroveň. Tato opatření jsou specifikována ve vztahu ke kvalitě (účinnosti) diagnostického systému modulu a ke snížení pravděpodobnosti vzniku nebezpečné události, které je ovlivněno také uspořádáním architektury hardware jednotlivých subsystémů. Skutečné technické řešení modulu UniAVV, resp. ostatních subsystémů automatického vedení vlaku musí být v souladu s uvedenými požadavky funkční bezpečnosti, aby bylo možné dosáhnout předpokládanou úroveň integrity bezpečnosti.

Z hlediska uspořádání architektury hardware jsou u modulu UniAVV a dalších subsystémů AVV použita následující řešení redundance jejich kanálů [5]:

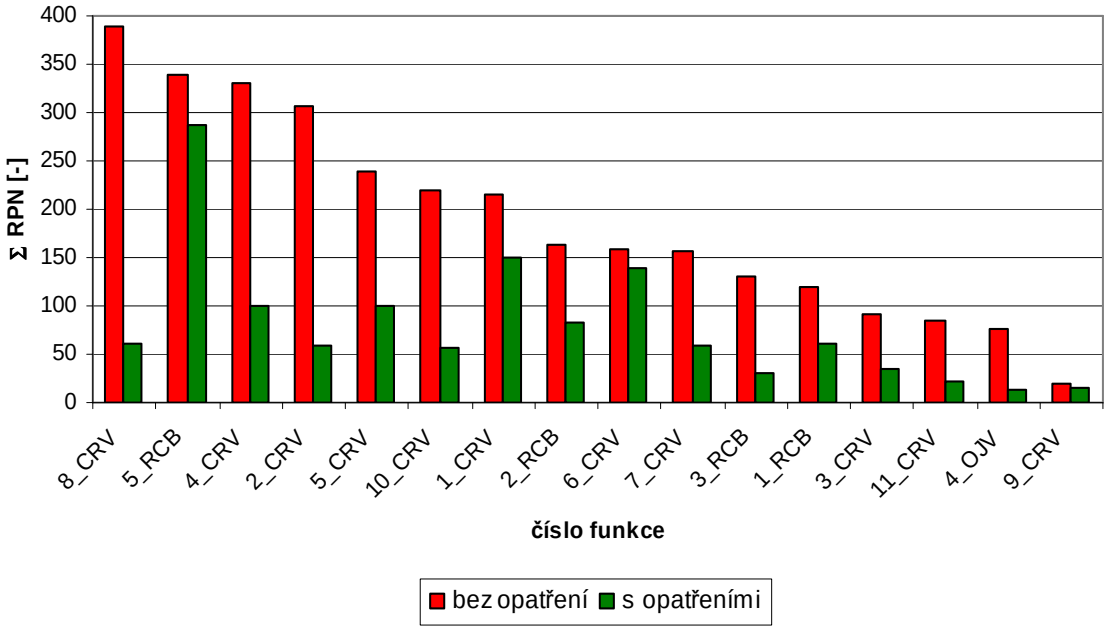
- Snímače rychlosti dvojkolí mají uspořádání architektury hardware 2oo4D, tzn. snímač rychlosti je umístěn na každém dvojkolí, pro měření a vyhodnocování rychlosti vozidla v režimech ARR, RCB a OJV musí být v provozuschopném stavu minimálně dva libovolné snímače. V případě zjištění poruchy snímače rychlosti dvojkolí je rozhodovací logika přizpůsobena správné činnosti funkce (po zásahu strojvedoucího vozidla).
- Blok logiky modulu UniAVV (procesorové desky, interní sběrnice CAN) má uspořádání architektury hardware 1oo2, tj. dva aktivní bloky jsou v paralelním uspořádání, požadované funkce může vykonávat každý z bloků, volbu provozního a záložního modulu provádí vozidlový počítač VTCU.

Důležitou vlastnost v souvislosti s principy funkční bezpečnosti představuje také nezávislost jednotlivých kanálů daného subsystému. U subsystému bloku logiky je u obou jednotek zajištěna jak nezávislost proti působení vnějších vlivů, tak i proti působení vnitřních fyzických a funkčních vlivů. Toho je dosaženo použitím řešení, kdy skříň každé jednotky je vybavena samostatným ventilátorem, je zajištěno galvanické oddělení vstupů, výstupů a napájení každé jednotky a mezi jednotkami neexistuje fyzické ani vnitřní komunikační propojení.

Z hlediska provádění automatických diagnostických testů jsou u modulu UniAVV a souvisejících subsystémů aplikována následující opatření, přispívající ke splnění požadavků funkční bezpečnosti [23]:

- procesorové desky tvořící blok logiky obsahují obvody watchdog, s napojením na bezpečnostní odpojovač výstupů,
- komunikační sběrnice CAN je v provedení se zabezpečeným komunikačním protokolem,
- provádění diagnostických selftestů snímačů rychlosti dvojkolí při sepnutí regulace vozidla (detekce zkratu, přerušení),
- provádění diagnostických selftestů snímače místních informačních bodů MIB při sepnutí regulace vozidla (funkce sepnutí snímače),
- použití cyklického zabezpečovacího kódu (CRC) pro zabezpečení přenosu signálu dvoubránovou pamětí RAM apod.

Aplikací výše uvedených opatření, navržených v souladu s požadavky funkční bezpečnosti, charakterizovanými určenou úrovní integrity bezpečnosti (SIL), by mělo být u modulu UniAVV dosaženo požadované redukce rizika na přípustnou úroveň. Ověření dosažené úrovně funkční bezpečnosti z kvalitativního hlediska hodnocení spolehlivosti je zajištěno opakovaným provedením analýzy způsobů a důsledků poruch (FMEA), s uvažováním opatření ke snížení rizika. Konkrétní výstupy z realizace této analýzy jsou uvedeny v tabulkách č. 5.12 a 5.13 (změny oproti počáteční analýze FMEA jsou kurzívou). Na obr. č. 5.4 je pak zobrazen graf porovnávající hodnoty Risk Priority Number (RPN) pro nejzávažnější funkce modulu UniAVV z počátečního a opakovaného provedení analýzy FMEA.



Obr. č. 5.4: Analýza FMEA – srovnání Risk Priority Number

Tabulka č. 5.12: Analýza FMEA (po opatření) – modul CRV

č.	Funkce	Způsob poruchy	Následek	Závažnost	Příčina	Výskyt	Detekce	RPN	Σ RPN
1	Určení rychlosti otáčení dvojkolí, výpočet okamžité rychlosti vozidla.	Ztráta požadované funkce.	Nelze zjistit hodnotu rychlosti vozidla. Nutnost odpojení modulu AVV a manuální řízení vozidla.	3	INP_01	***2***	***1***	***6***	***149***
					LOG_01	***1***	***1***	***3***	
		Chyba požadované funkce.	Skutečná rychlost je nižší než vypočtená rychlost. Možnost vzniku zpoždění.	5	LOG_02	1	***2***	***10***	
					MAN_01	2	3	30	
					INP_07	1	***2***	***10***	
		Chyba požadované funkce.	Skutečná rychlost je vyšší než vypočtená rychlost. Nebezpečí vykolejení.	9	LOG_02	1	***2***	***18***	
					MAN_01	2	3	54	
					INP_07	1	***2***	***18***	
2	Zajištění protismykové a protiskluzové ochrany (jednotlivých dvojkolí, synchronní).	Ztráta požadované funkce.	Neprovozuschopná protismyková a protiskluzová ochrana. Možnost vzniku zpoždění.	5	INP_01	***2***	***1***	***10***	***59***
					LOG_01	***1***	***1***	***5***	
					OUT_01	2	***1***	***10***	
					OUT_02	***1***	2	***10***	
		Chyba požadované funkce.	Změna hodnoty signálu PT+, PT- pro VTCU, resp. brzdič BSE.	6	LOG_02	1	***2***	***12***	
					OUT_04	1	***2***	***12***	
3	Regulace kladného poměrného tahu na základě požadavku (hl. jízdní páka, ARR).	Ztráta požadované funkce.	Nelze zadat požadovaný poměrný tah. Nutnost odpojení modulu AVV a manuální řízení vozidla.	3	INP_02	2	***1***	***6***	***35***
					LOG_01	***1***	***1***	***3***	
					OUT_01	2	***1***	***6***	
		Chyba požadované funkce.	Skutečná hodnota PT+ nižší než požadovaná. Možnost vzniku zpoždění.	5	LOG_02	1	***2***	***10***	
					OUT_04	1	***2***	***10***	
4	Regulace záporného poměrného tahu na základě požadavku (hl. jízdní páka, ARR).	Ztráta požadované funkce.	Není zajištěn požadovaný brzdný účinek. Nebezpečí vykolejení, projetí návěsti Stůj.	10	INP_02	***1***	***1***	***10***	***100***
					LOG_01	***1***	***1***	***10***	
					OUT_01	***1***	***1***	***10***	
					OUT_02	***1***	***1***	***10***	
		Chyba požadované funkce.	Nedostatečná hodnota PT-, nebezpečí vykolejení, projetí návěsti Stůj.	10	LOG_02	1	***2***	***20***	
					OUT_04	1	***2***	***20***	
					OUT_06	1	***2***	***20***	
5	Zajištění součinnosti pneumatické a elektrodynamické brzdy (vystřídací brzda).	Ztráta požadované funkce.	Nedostatečný brzdný účinek. Nebezpečí vykolejení, projetí návěsti Stůj.	10	INP_01	***2***	***1***	***20***	***100***
					LOG_01	***1***	***1***	***10***	
		Chyba požadované funkce.	Nedostatečný brzdný účinek. Nebezpečí vykolejení, projetí návěsti	10	LOG_02	1	5	50	
					INP_07	1	***2***	***20***	

Tabulka č. 5.12: Analýza FMEA (po opatření) – modul CRV, pokračování

6	Respektování délky vlaku ke konci pomalé jízdy.	Ztráta požadované funkce.	Nečinná funkce, nutný zásah strojvedoucího.	4	LOG_01	***1***	***1***	***4***	***139***
		Chyba požadované funkce.	Zrychlování vlaku v úseku pomalé jízdy. Nebezpečí vykolejení.	9	MAN_02	3	5	135	
7	Vyhodnocení signálů ze snímačů MIB.	Ztráta požadované funkce.	Nelze přesně identifikovat polohu vozidla. Aktivace brzdění vlaku, vznik	6	INP_03	***2***	***1***	***12***	***58***
					LOG_01	***1***	***1***	***6***	
		Chyba požadované funkce.	Nesprávná identifikace polohy vozidla. Nebezpečí projetí návěsti Stůj,	10	LOG_02	1	***2***	***20***	
					INP_04	1	***2***	***20***	
8	Zajištění mnohočlenného řízení vozidel v režimu AVV (přenos signálu PT).	Ztráta požadované funkce.	Není zajištěn přenos signálu PT do řízených vozidel. Nebezpečí	10	OUT_03	***1***	***1***	***10***	***60***
					LOG_01	***1***	***1***	***10***	
		Chyba požadované funkce.	Nesprávná hodnota signálu PT pro řízená vozidla. Nebezpečí vykolejení,	10	LOG_02	1	***2***	***20***	
					OUT_05	1	***2***	***20***	
9	Zajištění komunikace se strojvedoucím (klávesnice).	Ztráta požadované funkce.	Nelze zadat parametry pro ARR, RCB, OJV. Nutnost manuálního řízení	5	INP_05	***3***	***1***	***15***	***15***
					LOG_01	***1***	***1***	***5***	
10	Signalizace provozních informací ze systému AVV strojvedoucímu (displej).	Ztráta požadované funkce.	Strojvedoucí není informován o činnosti (nečinnosti) AVV. Odpojení	8	LOG_01	***1***	***1***	***8***	***56***
					OUT_01	***1***	***1***	***8***	
		Chyba požadované funkce.	Strojvedoucí je nesprávně informován o činnosti (nečinnosti) AVV. Nebezpečí vykolejení, projetí návěsti Stůj.	10	LOG_02	1	***2***	***20***	
					OUT_04	1	***2***	***20***	
11	Zajištění kontroly správných kombinací signálů, které umožňují jízdu vlaku.	Ztráta požadované funkce.	Nebezpečí poškození významných konstrukčních celků vozidla.	7	LOG_01	***1***	***1***	***7***	***21***
		Chyba požadované funkce.	Nebezpečí poškození významných konstrukčních celků vozidla.	7	LOG_02	1	***2***	***14***	

Tabulka č. 5.13: Analýza FMEA (po opatření) – moduly RCB a OJV

č.	Funkce	Způsob poruchy	Následek	Závažnost	Příčina	Výskyt	Detekce	RPN	Σ RPN
1	Idenfitikace polohy vozidla na trati.	Chyba požadované funkce.	Nelze přesně identifikovat polohu vozidla. Nebezpečí vykolejení, projetí návěsti Stůj.	10	EXT_02	1	***1***	***10***	***60***
					MAN_01	2	***1***	***20***	
					MAN_03	3	***1***	***30***	
2	Načítání dat z palubní mapy tratě a palubního jízdního řádu.	Ztráta požadované funkce.	Nejsou k dispozi potřebná data. Nutnost aktivace režimu ARR nebo MAN.	3	LOG_01	***1***	***1***	***3***	***83***
		Chyba požadované funkce.	Načítání nesprávných dat. Nebezpečí vykolejení, projetí návěsti Stůj.	10	EXT_03	1	***3***	***30***	
					MAN_03	3	***1***	***30***	
					LOG_02	1	***2***	***20***	
3	Realizace cílového brzdění (výpočet požadované rychlosti pro ARR v závislosti na poloze).	Ztráta požadované funkce.	Není realizováno cílové brzdění. Nebezpečí vykolejení nebo projetí návěsti Stůj.	10	LOG_01	***1***	***1***	***10***	***30***
		Chyba požadované funkce.	Chybná hodnota požadované rychlosti. Nebezpečí vykolejení nebo projetí návěsti Stůj.	10	LOG_02	1	***2***	***20***	
4	Realizace energeticky optimální jízdní strategie.	Ztráta požadované funkce.	Není realizována energeticky optimální jízda.	3	LOG_01	***1***	***1***	***3***	***13***
		Chyba požadované funkce.	Chybně realizovaná energeticky optimální jízda. Možnost vzniku zpoždění.	5	LOG_02	1	***2***	***10***	
5	Vyhodnocování kódu mobilní části vlakového zabezpečovače.	Ztráta požadované funkce.	Vozidlo realizuje cílové brzdění podle nejzávažnějšího možného návěstního	6	INP_06	2	***1***	***12***	***288***
					LOG_01	***1***	***1***	***6***	
		Chyba požadované funkce.	Cílové brzdění k nesprávné návěsti oproti VZ. Nebezpečí vykolejení, projetí	10	LOG_02	1	***2***	***20***	
					MAN_04	5	5	250	

U funkcí, jež jsou realizovány pouze prostřednictvím subsystémů modulu UniAVV, došlo po aplikaci technických opatření podle požadavků funkční bezpečnosti k výraznému snížení rizika, charakterizované poklesem hodnoty indexu RPN. Ke snížení hodnoty Risk Priority Number nedošlo pouze u funkcí, jejichž selhání může být způsobeno chybou lidského činitele (zadání neodpovídající rychlosti pro vícepovolující návěstní znaky nebo chybné zadání délky vlaku strojvedoucím, případně chybné zadání poloměru kol vozidla pracovníky údržby).

Nebezpečí spojené se selháním lidského činitele v souvislosti s činností modulu UniAVV je možné redukovat pouze aplikací vnějšího ochranného systému, jehož přispěním by bylo možné detekovat nesprávnou činnost systému AVV, vyvolanou vnějším faktorem, a provést taková opatření, která by zabránila vzniku nebezpečné situace.

Takový typ nezávislého systému představuje jednotný evropský zabezpečovací systém v železniční dopravě – ETCS (European Train Control System). Jednou z funkcí tohoto systému je vyhodnocování okamžité rychlosti vlaku na základě přenášeného statického rychlostního profilu, který zohledňuje aktuální situaci (polohu vlaků, stav návěstidel, omezení rychlosti) na dané trati. V případě, že dojde k překročení vypočtené nejvyšší dovolené rychlosti v daném okamžiku, je prostřednictvím systému ETCS aktivován brzdový systém vlaku. Tento systém tedy zasáhne také v případech, kdy vlivem chyby lidského činitele dojde k selhání funkce modulu UniAVV (v manuálním nebo automatickém režimu řízení) a vlak se pohybuje rychlostí vyšší než je v daném okamžiku rychlost dovolená. Konstrukce modulu UniAVV navíc umožňuje aktivní spolupráci se zabezpečovacím systémem ETCS, kdy od něho může přejímat kompletní statický rychlostní profil tratě. V tomto případě je eliminována možnost vzniku chyby strojvedoucího při zadávání rychlosti pro vícepovolující návěstní znaky v současné době používaného vlakového zabezpečovače LVZ.

Aby použitím zabezpečovacího systému ETCS došlo k efektivní redukci rizika spojeného s vlivem lidského činitele při automatickém vedení vlaku, je nutné, aby tento systém dosáhl požadované úrovně z hlediska funkční bezpečnosti. Systém ETCS tak musí splňovat minimálně takovou úroveň integrity bezpečnosti (SIL), která je požadována pro funkce modulu UniAVV, jež jsou při současném řešení spojeny s činností lidského činitele.

6 KVANTITATIVNÍ HODNOCENÍ SPOLEHLIVOSTI MODULU UniAVV

Pro zajištění bezpečného a spolehlivého provozu železniční dopravy je nutné, aby systémy železničních vozidel splňovaly kritéria daná příslušnými normami, či jinými právními předpisy. Modul UniAVV, který je centrální výkonnou, řídicí a diagnostickou jednotkou systému automatického vedení vlaku (AVV), je vhodné z tohoto hlediska posuzovat v souvislosti s principy funkční bezpečnosti jako elektrický/elektronický systém související s bezpečností. Pro stanovenou požadovanou úroveň integrity bezpečnosti (SIL) systému AVV, která byla určena na základě kvalitativního hodnocení rizik spojených s činností systému, je nezbytné její prokázání provedením kvantitativní analýzy s cílem určení konkrétních číselných charakteristik spolehlivosti systému.

6.1 Teoretický model spolehlivosti – systém AVV

Pro možnost určení konkrétních hodnot kvantitativních ukazatelů spolehlivosti systému automatického vedení vlaku (AVV) je nezbytné vytvoření jeho teoretického modelu spolehlivosti. Vzhledem k požadavkům na spolehlivost systému, vyjádřeným ve formě požadované úrovně integrity bezpečnosti (SIL), je model spolehlivosti koncipován v souladu s principy funkční bezpečnosti s důrazem na nebezpečné poruchy systému AVV, které mohou vyvolat ohrožení bezpečnosti železniční dopravy.

Z výše uvedeného důvodu hodnotí model spolehlivosti především bezporuchovost (resp. pravděpodobnost poruchy) systému automatického vedení vlaku. Další ukazatele spolehlivosti, tj. udržovatelnost a zajištěnost údržby, nejsou v tomto modelu uvažovány. Při provádění údržby a oprav součástí systému AVV se nepředpokládá jeho činnost automatického řízení jízdy vozidla, a proto po tuto dobu nemůže vzniknout ohrožení bezpečnosti.

Teoretický model bezporuchovosti systému AVV je sestaven za předpokladu, že riziko spojené s ohrožením bezpečnosti provozu železniční dopravy způsobí taková porucha systému AVV, o které není obsluha vozidla informována prostřednictvím diagnostického systému. Z tohoto hlediska je model vytvořen pro nebezpečné nediagnostikované poruchy

systému AVV s cílem určení typických charakteristik bezporuchovosti, resp. funkční bezpečnosti, a výpočtu jejich konkrétních číselných hodnot.

Teoretický model je konstruován pro náhodné poruchy hardware, tvořícího systém AVV, za předpokladu, že pracuje ve funkčně nejnáročnějším režimu cílového brzdění (CB) s případnou optimalizací jízdy vlaku (OJV). Pro jeho sestavení je využito analýzy stromu poruchových stavů (FTA), jejíž postup a vyhodnocení jsou popsány v [1], [2].

Sestavení stromu poruch vede od vrcholové události postupně k poruchám na nižších úrovních systému a následně je provedena kvantifikace jejich pravděpodobností [1]. Vrcholovou událost u systému automatického vedení vlaku představuje nebezpečná nediagnostikovaná porucha. V teoretickém modelu, bez zpřesňujících podmínek, tato porucha vzniká v případě, že vznikne nebezpečná porucha funkce systému AVV a současně porucha diagnostického systému, který je určen k detekování poruch systému AVV. Rozvoj stromu poruch je uveden na obr. č. 6.1.

Nebezpečná porucha funkce systému AVV představuje poruchu některého z hlavních subsystémů systému (tj. porucha vstupních signálů, porucha bloku provádějícího logické operace nebo porucha výstupních signálů), která může způsobit ohrožení bezpečnosti.

Hardware subsystému vstupních signálů, který přenáší informace o rychlosti a poloze vozidla, stavu traťového zabezpečovacího zařízení a požadavcích strojvedoucího, je s výjimkou snímačů otáček dvojkolí řešen jako jednokanálová architektura. Při poruše přenosu signálu vlakového zabezpečovače (LVZ), poruše snímače informačních bodů na trati (MIB) nebo poruše hlavní jízdní páky není možné jejich funkce nahradit a systém AVV nemůže vykonávat požadovanou činnost. Hardware přenosu signálu otáček dvojkolí má vícekanálové uspořádání architektury, kdy snímač otáček je umístěn na každém dvojkolí. Signály jednotlivých snímačů jsou porovnávány a vyhodnocovány diagnostickým systémem AVV a pro správnou činnost je dostačující, když je v činnosti libovolná kombinace alespoň dvou snímačů ze všech čtyřech. Tato architektura tedy představuje uspořádání typu „*m* z *n*“ (2 ze 4, podle norem funkční bezpečnosti označení 2oo4D).

Subsystém zpracovávající logické operace systému AVV (blok logiky) je v konstrukčním řešení lokomotivy řady 109E (ř. 380) proveden v redundantním uspořádání. Je tvořen dvěma identickými bloky, přičemž v činnosti jsou oba bloky současně, i když požadované funkce vykonává vždy pouze jeden z nich. Toto provedení představuje tzv. horkou zálohu. O volbě aktivního, resp. pasivního (záložního) bloku logiky rozhoduje

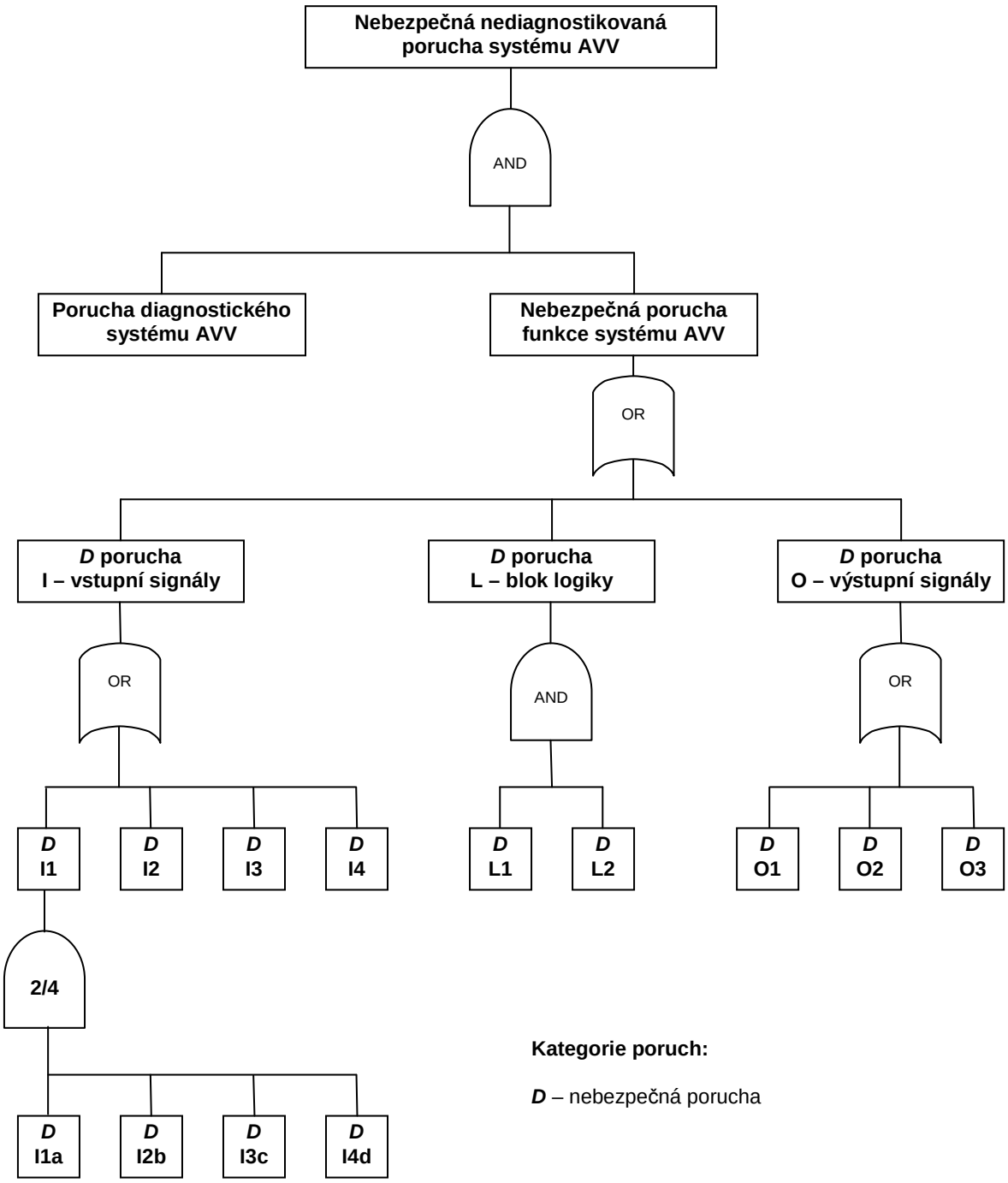
vozidlový počítač lokomotivy (VTCU). Na základě diagnostických testů, které vyhodnocují a porovnávají signály a stavy obou bloků, může vozidlový počítač aktivní blok z důvodu poruchy odpojit a okamžitě nahradit blokem záložním [23]. Z hlediska architektury hardware toto uspořádání představuje dvoukanálovou architekturu s označením 1oo2.

Výstupní signály systému AVV představují signály pro akční členy, jejichž prostřednictvím je vozidlo řízeno v automatickém režimu jízdy. Patří k nim signál pro vozidlový počítač (signál regulace výkonu, signál pro zobrazovací monitor), signál pro ovládání elektrického brzdiče lokomotivy (BSE) a signál pro mnohočlenné řízení vozidel. Architektura hardware přenosu těchto signálů je řešena jako jednokanálová, tedy při poruše kanálu dochází k poruše požadované funkce a systém AVV nemůže provádět svoji činnost.

Diagnostický systém pro detekci poruch systému AVV je v tomto obecném případě řešen jako plně nezávislý na systému AVV, se schopností detekovat všechny u něho vzniklé poruchy. V tomto případě dochází k nebezpečné nediagnostikované poruše pouze, pokud porucha funkce systému AVV a porucha diagnostického systému nastanou současně. Avšak v technické praxi je obvyklé, že diagnostické systémy jsou součástí řídicího systému sledovaného objektu a technicky není možné diagnostikovat všechny vzniklé poruchy systému.

Tento přístup je také využit u systému AVV, resp. modulu UniAVV. Z hlediska funkční bezpečnosti představuje modul UniAVV řízené zařízení (EUC) a současně systém řízení EUC. Zároveň tento modul provádí také diagnostické testy systému AVV, a tedy jeho součástí je i systém související s bezpečností, který tudíž není na modulu UniAVV nezávislý. V tomto smyslu je dle požadavků funkční bezpečnosti nezbytné považovat jak řízené zařízení (EUC), tak také systém řízení EUC za systém související s bezpečností.

Nediagnostikované poruchy vznikají u systému AVV jednak při poruše subsystému modulu UniAVV, který provádí detekci poruch, ale také z důvodu, že diagnostický systém poruchu není schopný detekovat vlivem své konstrukce a funkcí, které může vykonávat. Schopnost diagnostického systému detekovat poruchy je charakterizována parametrem diagnostického pokrytí, který udává, jaký podíl poruch je diagnostický systém schopný zjistit. Dalším faktorem, který ovlivňuje možnost detekce poruch, je interval provádění automatických diagnostických testů. S rostoucím intervalem těchto testů se zvyšuje pravděpodobnost nediagnostikované poruchy, i když je diagnostický systém v provozuschopném stavu.



Kategorie poruch:

D – nebezpečná porucha

I – vstupní signály:

I1 – signál otáček dvojkolí
I1a, I1b, I1c, I1d – snímače otáček 1.-4. dvojkolí

I2 – signál poměrný tah (hl. jízdní páka)
I3 – signál snímače MIB
I4 – signál LVZ

L – blok logiky:

L1 – aktivní blok logiky
L2 – záložní blok logiky

O – výstupní signály:

O1 – signál do VTCU (vozidlový počítač)
O2 – signál pro BSE
O3 – signál mnohočlenného řízení

Obr. č. 6.1: Strom poruch systému AVV, obecný přístup

Výše uvedené důvody vedou k závěru, že uvedený teoretický model, předpokládající nezávislost diagnostického systému a vznik nediagnostikované poruchy pouze při náhodné poruše diagnostického systému, není pro systém AVV vhodný. Přesto je níže uveden postup určení vztahu pro nebezpečnou nediagnostikovanou, resp. nebezpečnou poruchu, vycházející ze stromu poruch na obr. č. 6.1. Tento vztah bude využit u sestavování následujícího teoretického modelu.

Nebezpečná nediagnostikovaná porucha v tomto případě nastává, když nastane současně nebezpečná porucha funkce systému AVV, s pravděpodobností F_D, a porucha diagnostického systému, daná pravděpodobností F_U. Pravděpodobnost nebezpečné nediagnostikované poruchy F_{DU} je vyjádřena jako součin uvedených pravděpodobností:

$$F_{DU} = F_D \cdot F_U \quad [-] \tag{6.1}$$

Nebezpečná porucha funkce systému AVV nastane v případě, že dojde k nebezpečné poruše některého z jeho subsystémů (vstupní signály, výstupní signály nebo oba bloky logiky). Pravděpodobnost této poruchy F_D je možné vyjádřit vztahem:

$$F_D = 1 - (1 - F_{D-I}) \cdot (1 - F_{D-L}) \cdot (1 - F_{D-O}) \quad [-] \tag{6.2}$$

kde: $F_{D\text{-}I}$ – pravděpodobnost nebezpečné poruchy subsystému vstupních signálů [-],
$F_{D\text{-}L}$ – pravděpodobnost nebezpečné poruchy subsystému bloků logiky [-],
$F_{D\text{-}O}$ – pravděpodobnost nebezpečné poruchy subsystému výstupních signálů [-].

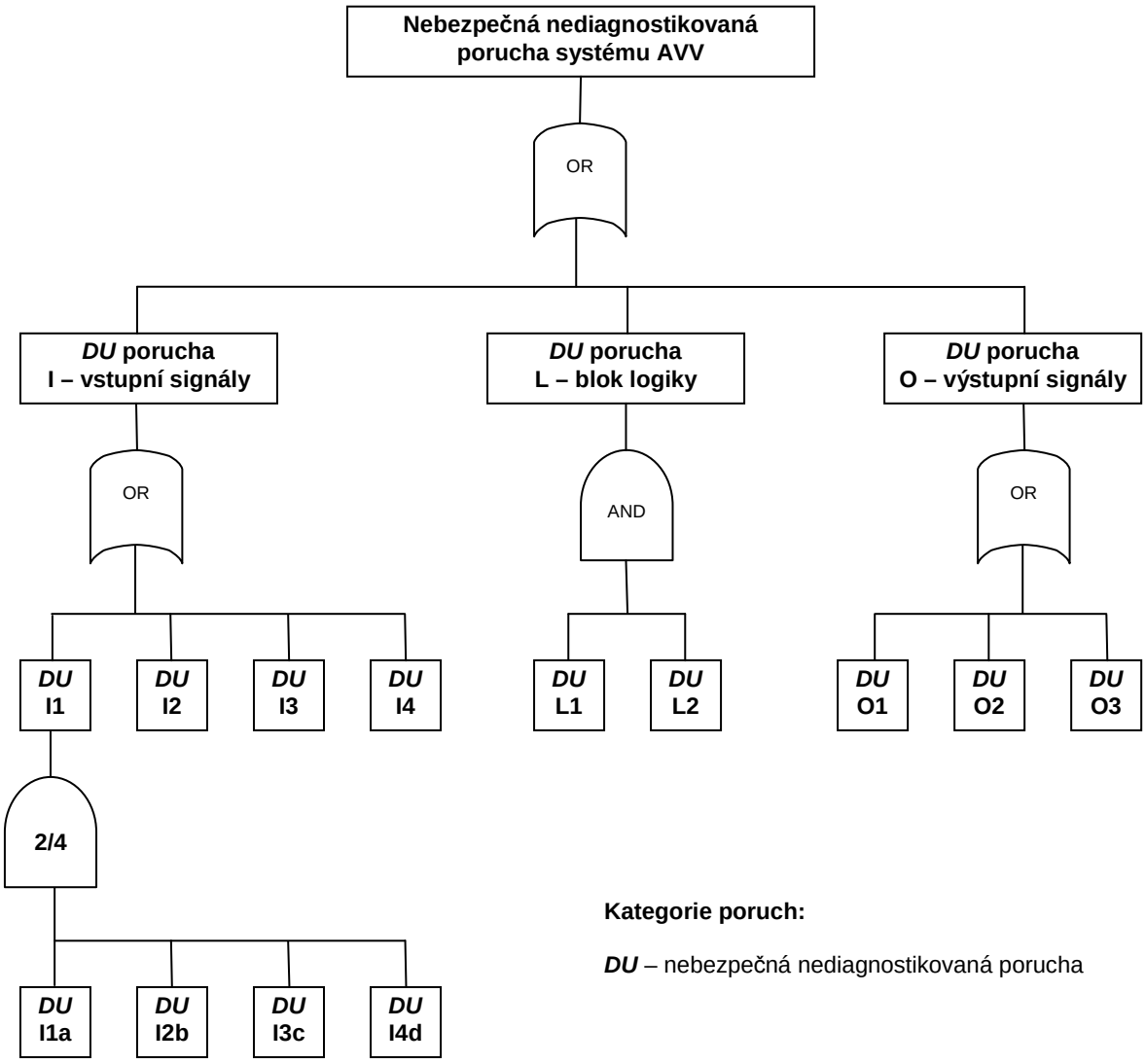
Tuto rovnici je možné dále rozvinout pro jednotlivé vstupní a výstupní signály, resp. aktivní a záložní blok logiky. Za předpokladu, že k nebezpečné poruše dojde při poruše některého ze vstupních nebo výstupních signálů, nebo při poruše obou bloků logiky, lze vztah zapsat:

$$F_D = 1 - \left[\prod_{i=1}^{4}(1 - F_{D-Ii})\right] \cdot \left[1 - \prod_{j=1}^{2} F_{D-Lj}\right] \cdot \left[\prod_{k=1}^{3}(1 - F_{D-Ok})\right] \quad [-] \tag{6.3}$$

Ve výše uvedeném stromu poruch se subsystémy nerozvíjejí do nižších úrovní, s výjimkou signálu otáček dvojkolí. Tento kanál má uspořádání hardware typu „*m* z *n*“. Pro pravděpodobnost nebezpečné poruchy signálu otáček dvojkolí $F_{D\text{-}I1}$, vyjádřenou pomocí pravděpodobnosti nebezpečné poruchy jednotlivých snímačů otáček $F_{D\text{-}I1x}$, za předpokladu, že jsou totožné, platí:

$$F_{D-I1} = 1 - \sum_{m=2}^{4} \binom{4}{m} \cdot (1 - F_{D-I1x})^m \cdot (F_{D-I1x})^{4-m} \quad [-] \tag{6.4}$$

Dosazením vztahu (6.4) do vztahu (6.3) se získá vztah popisující pravděpodobnost nebezpečné poruchy funkce systému AVV na úrovni jeho subsystémů.



I – vstupní signály:

I1 – signál otáček dvojkolí
I1a, I1b, I1c, I1d – snímače otáček 1.-4. dvojkolí

I2 – signál poměrný tah (hl. jízdní páka)
I3 – signál snímače MIB
I4 – signál LVZ

L – blok logiky:

L1 – aktivní blok logiky
L2 – záložní blok logiky

O – výstupní signály:

O1 – signál do VTCU (vozidlový počítač)
O2 – signál pro BSE
O3 – signál mnohočlenného řízení

Obr. č. 6.2: Strom poruch systému AVV, skutečný stav

Upravený teoretický model bezporuchovosti pro nebezpečnou nediagnostikovanou poruchu systému AVV, vycházející z rozvoje stromu poruch na obr. č. 6.2, zohledňuje skutečné pojetí diagnostického systému a možnost provádění detekce nebezpečných poruch modulem UniAVV. Nediagnostikovaná porucha tak může vzniknout nejen vlivem poruchy diagnostického systému, ale také jeho nedokonalostí a trváním intervalu mezi provedením automatických diagnostických testů. Tyto faktory mají vliv na pravděpodobnost nedetekování nebezpečné poruchy funkce systému AVV a tato pravděpodobnost je určena zvlášť pro každý subsystém uvedený ve stromu poruch.

Vztah pro pravděpodobnost nebezpečné nediagnostikované poruchy systému AVV F_{DU} lze pak zapsat s využitím vztahu (6.3), kdy každá dílčí pravděpodobnost nebezpečné poruchy funkce subsystému je ovlivněna pravděpodobností, s jakou nelze danou poruchu detekovat, neboli:

$$F_{DU} = 1 - \left(1 - F_{D-I} \cdot F_{U-I}\right) \cdot \left(1 - F_{D-L} \cdot F_{U-L}\right) \cdot \left(1 - F_{D-O} \cdot F_{U-O}\right) \qquad [-] \tag{6.5}$$

kde: $F_{D\text{-}I}$ – pravděpodobnost nebezpečné poruchy subsystému vstupních signálů [-],
$F_{D\text{-}L}$ – pravděpodobnost nebezpečné poruchy subsystému bloků logiky [-],
$F_{D\text{-}O}$ – pravděpodobnost nebezpečné poruchy subsystému výstupních signálů [-],
$F_{U\text{-}I}$ – pravděpodobnost nedetekování nebezpečné poruchy subsystému vstupních signálů [-],
$F_{U\text{-}L}$ – pravděpodobnost nedetekování nebezpečné poruchy subsystému bloků logiky [-],
$F_{U\text{-}O}$ – pravděpodobnost nedetekování nebezpečné poruchy subsystému výstupních signálů [-].

V případě rozvoje subsystémů na úroveň jednotlivých vstupních a výstupních signálů, resp. dvou bloků logiky, přejde vztah (6.5) do tvaru:

$$F_{DU} = 1 - \left[\prod_{i=1}^{4}\left(1 - F_{D-Ii} \cdot F_{U-Ii}\right)\right] \cdot \left[1 - \prod_{j=1}^{2} F_{D-Lj} \cdot F_{U-Lj}\right] \cdot \left[\prod_{k=1}^{3}\left(1 - F_{D-Ok} \cdot F_{U-Ok}\right)\right] \tag{6.6}$$

Vztah pro pravděpodobnost nebezpečné nediagnostikované poruchy signálu otáček dvojkolí $F_{DU\text{-}I1}$ se určí analogicky s využitím binomického rozdělení pro systémy typu „*m* z *n*“ jako u předchozího modelu ve vztahu (6.4).

Vzhledem ke skutečnosti, že modul UniAVV vykonává jak funkce systému řízení EUC, tak také funkce systému souvisejícího s bezpečností (diagnostický systém), nejsou tyto dva systémy oddělené a nezávislé (jak je uvedeno výše). Rovnice (6.6) tak přechází do tvaru, kde pravděpodobnost nebezpečné nediagnostikované funkce jednotlivých subsystémů systému AVV je charakterizována jedinou číselnou hodnotou. Pravděpodobnost nebezpečné

nediagnostikované poruchy systému AVV F_{DU} s uvážením jednotlivých subsystémů uvedených ve stromu poruch na obr. č. 6.2, tj. vstupních a výstupních signálů a dvou bloků logiky, je:

$$F_{DU} = 1 - \left[\prod_{i=1}^{4}\left(1 - F_{DU-Ii}\right)\right] \cdot \left[1 - \prod_{j=1}^{2} F_{DU-Lj}\right] \cdot \left[\prod_{k=1}^{3}\left(1 - F_{DU-Ok}\right)\right] \quad [-] \tag{6.7}$$

V dosavadním modelu bezporuchovosti systému AVV byly uvažovány konstantní pravděpodobnosti poruch jednotlivých subsystémů. V technické praxi však obvykle mají tyto charakteristiky časově závislý průběh s konkrétním typem a parametry rozdělení pravděpodobnosti náhodné veličiny. Rovnici (6.7), vyjadřující pravděpodobnost nebezpečné nediagnostikované poruchy systému AVV, lze v tomto případě zapsat jako distribuční funkci náhodné veličiny, neboli:

$$F_{DU}(t) = 1 - \left[\prod_{i=1}^{4}\left(1 - F_{DU-Ii}(t)\right)\right] \cdot \left[1 - \prod_{j=1}^{2} F_{DU-Lj}(t)\right] \cdot \left[\prod_{k=1}^{3}\left(1 - F_{DU-Ok}(t)\right)\right] \tag{6.8}$$

Systém AVV je složen ze subsystémů tvořených elektrickými a elektronickými prvky. U tohoto typu součástí je obvyklé, že náhodná veličina, kterou představuje doba do poruchy součásti, má exponenciální rozdělení pravděpodobnosti. Toto rozdělení je charakterizováno jediným parametrem λ [h^{-1}], tedy intenzitou poruch, která je pro toto rozdělení konstantní [6].

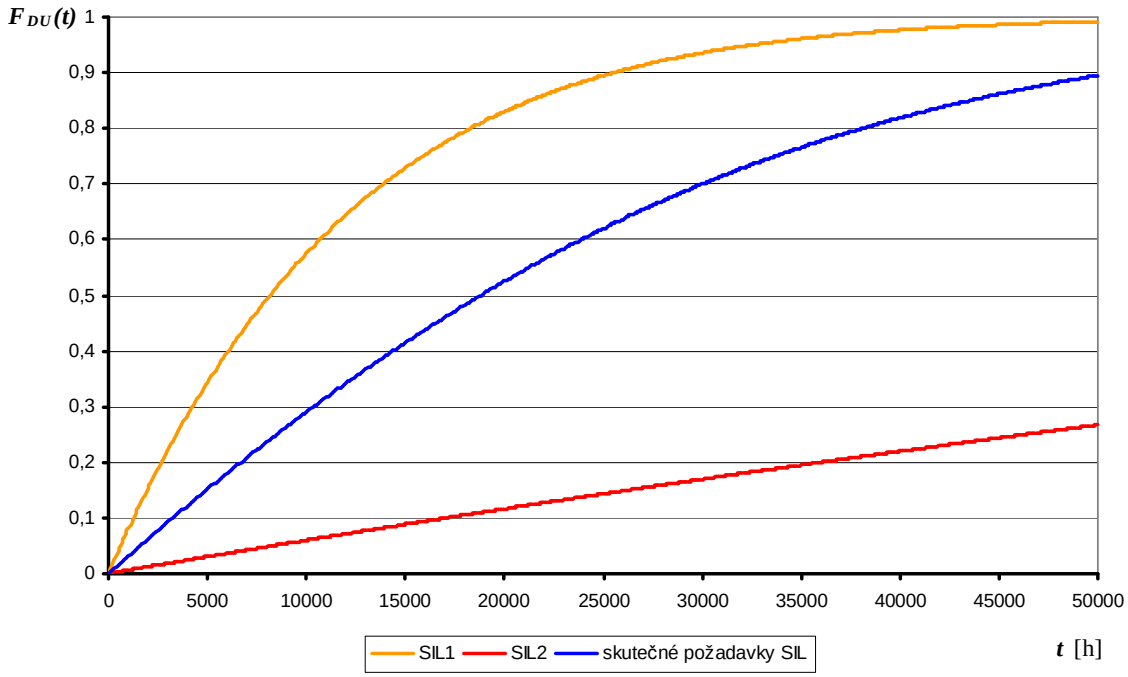
Pravděpodobnost nebezpečné nediagnostikované poruchy subsystému souvisejícího s bezpečností je tedy vyjádřena jako funkce doby provozu zařízení. Během provozu systému AVV mohou vzniknout nebezpečné poruchy, které budou diagnostikovány až při dalším provedení automatického diagnostického testu, v okamžiku vzniku poruchy je tedy nelze detekovat. Některé nebezpečné poruchy systému AVV nelze detekovat žádným způsobem vlivem ne zcela dokonalého diagnostického systému a tyto poruchy jsou zjištěny až při vyžádání bezpečnostní funkce v průběhu doby životnosti zařízení.

Z uvedených faktorů ovlivňujících vznik nediagnostikovaných poruch vychází vztah pro pravděpodobnost nebezpečné nediagnostikované poruchy pro exponenciální rozdělení pravděpodobnosti náhodné veličiny. Pro jednotlivé subsystémy systému AVV, uvedené ve stromu poruch na obr. č. 6.2 je tento vztah identický, liší se pouze jeho konkrétní parametry. Například pro *i*-tý subsystém vstupních signálů je pravděpodobnost nebezpečné nediagnostikované poruchy $F_{DU\text{-}Ii}(t)$ dána vztahem:

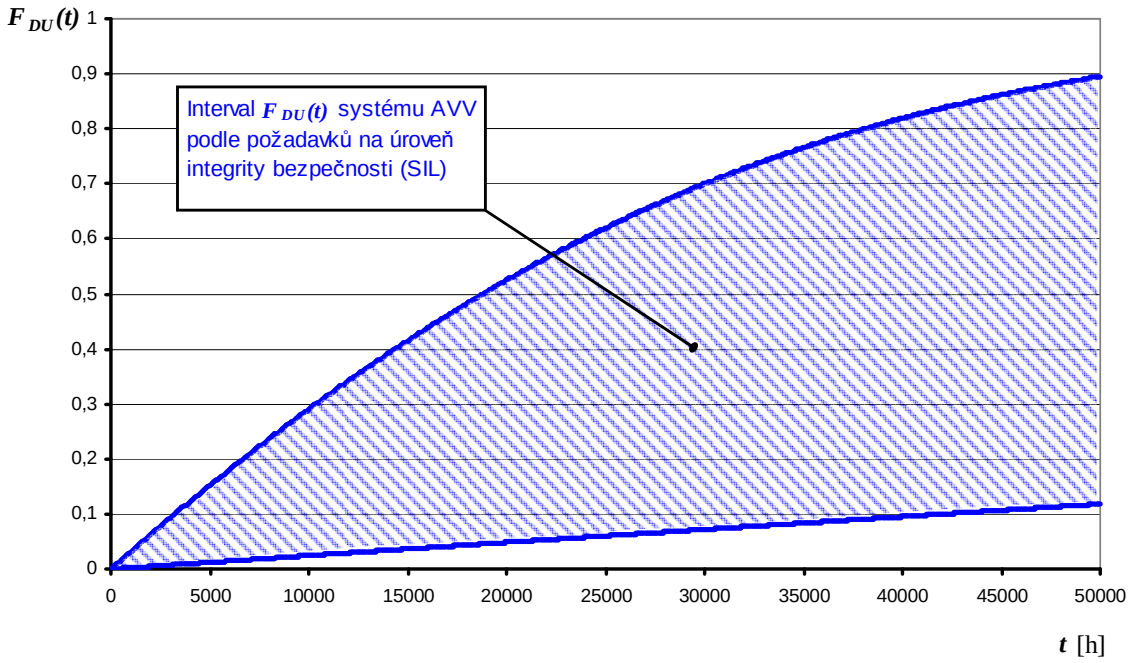
$$F_{DU-Ii}(t) = 1 - \exp\left[-\left(\lambda_{DD-Ii} \cdot t_{PT-Ii} + \lambda_{DU-Ii} \cdot t_{LT-Ii}\right)\right] \qquad [-] \tag{6.9}$$

kde:
- $\lambda_{DD\text{-}Ii}$ – intenzita nebezpečných diagnostikovaných poruch *i*-tého subsystému vstupů [h^{-1}],
- $\lambda_{DU\text{-}Ii}$ – intenzita nebezpečných nediagnostikovaných poruch *i*-tého subsystému vstupů [h^{-1}],
- $t_{PT\text{-}Ii}$ – interval provádění automatických diagnostických testů *i*-tého subsystému vstupních signálů [h],
- $t_{LT\text{-}Ii}$ – doba provozu *i*-tého subsystému vstupních signálů, resp. systému AVV jako celku [h].

Pokud jsou známy konkrétní hodnoty výše uvedených parametrů jednotlivých subsystémů, lze určit jednotlivé charakteristiky náhodné veličiny, vycházející z teoretického modelu spolehlivosti systému AVV. Na obr. č. 6.3 je znázorněn průběh pravděpodobnosti nebezpečné nediagnostikované poruchy $F_{DU}(t)$ systému AVV pro předpokládanou dobu životnosti zařízení 50 000 hodin. Graf znázorňuje maximální možnou pravděpodobnost poruchy, které může systém AVV dosáhnout, aby byly splněny požadavky na úroveň integrity bezpečnosti (SIL) jednotlivých subsystémů, definované s využitím kvalitativního hodnocení rizika. Pro srovnání je uveden průběh maximální možné pravděpodobnosti nebezpečné nediagnostikované poruchy systému za předpokladu, že jeho jednotlivé subsystémy splňují požadavek na úroveň integrity bezpečnosti SIL1, resp. SIL2.



Obr. č. 6.3: Pravděpodobnost $F_{DU}(t)$ systému AVV, srovnání rozdílných SIL



Obr. č. 6.4: Interval pravděpodobnosti $F_{DU}(t)$ systému AVV podle požadavků na SIL

V grafu na obr. č. 6.4 je zobrazen průběh maximální možné pravděpodobnosti a minimální definované pravděpodobnosti nebezpečné nediagnostikované poruchy systému AVV, pokud jeho jednotlivé subsystémy splňují požadavky na úroveň integrity bezpečnosti (SIL), pro předpokládanou životnost zařízení 50 000 hodin. Tyto dvě křivky tak vymezují oblast, ve které se bude nacházet skutečný průběh pravděpodobnosti nebezpečné nediagnostikované poruchy systému AVV, pokud jednotlivé subsystémy budou mít takové parametry spolehlivosti, kterými vyhoví požadavkům na ukazatele funkční bezpečnosti charakterizujícím danou úroveň integrity bezpečnosti (SIL).

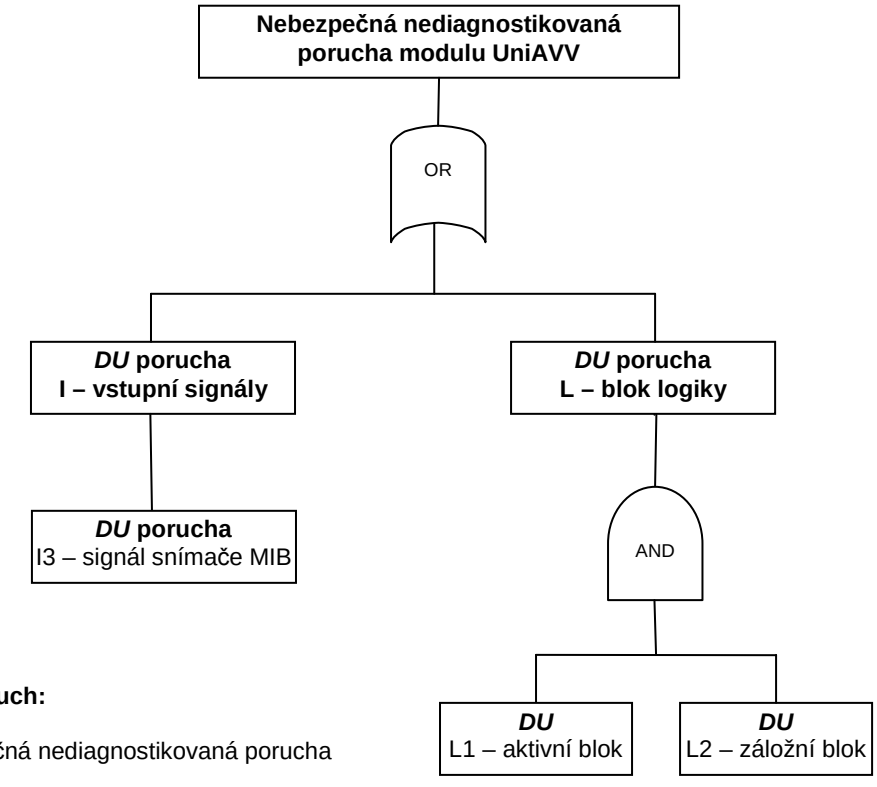
6.2 Teoretický model spolehlivosti – modul UniAVV

Systém automatického vedení vlaku (AVV) představuje konstrukčně složité zařízení, složené z velkého počtu subsystémů, jejichž vývoj a výroba není z důvodu konstrukční variability zajišťována pouze jedním výrobcem. Jednotliví výrobci odpovídají u vlastních zařízení za dosažení takových parametrů spolehlivosti, aby systém AVV jako celek splnil požadavky dané technickou dokumentací, právními a normativními předpisy, smluvními podmínkami odběratele apod.

Základním konstrukčním celkem systému AVV je modul UniAVV, jehož vývoj a výrobu provádí společnost MSV elektronika s.r.o. Tento modul realizuje samotnou úlohu automatického vedení vlaku, provádí identifikaci polohy vozidla na trati a také zajišťuje výkon funkcí souvisejících s bezpečností prostřednictvím vlastního diagnostického systému. Modul UniAVV tedy obsahuje subsystém bloku provádějícího logické operace a subsystém přenosu signálu o poloze vozidla na trati (informační body na trati – MIB).

Teoretický model spolehlivosti modulu UniAVV vychází z výše uvedeného modelu pro systém AVV jako celek. Pro jeho sestavení je využit rozvoj stromu poruch, který určuje příčiny vzniku nebezpečné nediagnostikované poruchy modulu UniAVV (viz obr. č. 6.5). Z analýzy stromu poruch vyplývá, že tato porucha může nastat u modulu UniAVV ve dvou případech:

- nebezpečná porucha funkce bloku logiky, kterou nelze detekovat; porucha nastává z důvodu redundantního uspořádání při poruše obou bloků logiky (aktivního a záložního);
- nebezpečná porucha funkce přenosu signálu ze snímače MIB, kterou nelze detekovat; z důvodu jednokanálového uspořádání nemůže subsystém vykonávat požadovanou funkci při vzniku jedné poruchy.



Obr. č. 6.5: Strom poruch, modul UniAVV

Vyčleněním uvedených subsystémů z teoretického modelu pro systém AVV lze sestavit model spolehlivosti pro samotný modul UniAVV. Tento model, shodně jako výše uvedený model, je charakterizován pravděpodobností nebezpečné nediagnostikované poruchy F_{DU}:

$$F_{DU} = 1 - (1 - F_{DU-I3}) \cdot (1 - F_{DU-L1} \cdot F_{DU-L2}) \quad [-] \tag{6.10}$$

kde: F_{DU} – pravděpodobnost nebezpečné nediagnostikované poruchy modulu UniAVV [-],
$F_{DU\text{-}I3}$ – pravděpodobnost nebezpečné nediagnostikované poruchy subsystému signálu snímače MIB [-],
$F_{DU\text{-}L1}$ – pravděpodobnost nebezpečné nediagnostikované poruchy subsystému bloku logiky 1 (aktivní blok) [-],
$F_{DU\text{-}L2}$ – pravděpodobnost nebezpečné nediagnostikované poruchy subsystému bloku logiky 2 (záložní blok) [-].

Při předpokladu časově proměnných pravděpodobností, kdy jejich hodnoty jsou závislé na době provozu systému, přechází vztah (6.10) do tvaru, kdy pravděpodobnost $F_{DU}(t)$ vyjadřuje distribuční funkci náhodné veličiny, tj. doby do nebezpečné nediagnostikované poruchy:

$$F_{DU}(t) = 1 - [1 - F_{DU-I3}(t)] \cdot [1 - F_{DU-L1}(t) \cdot F_{DU-L2}(t)] \quad [-] \tag{6.11}$$

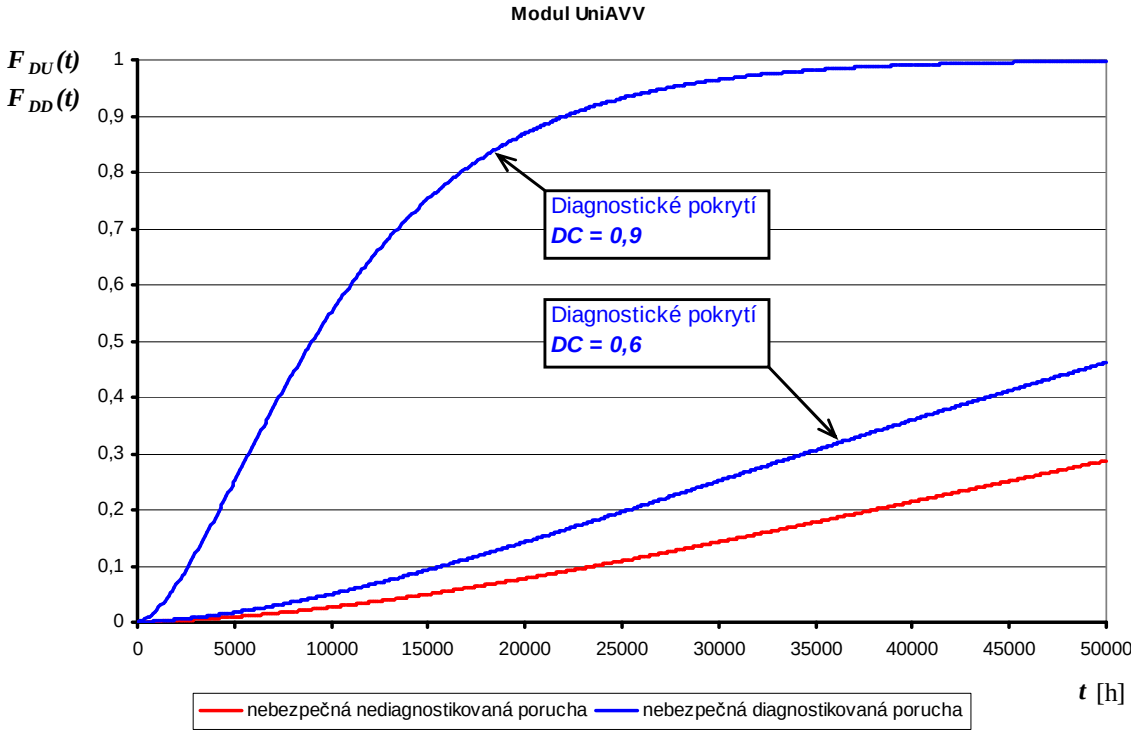
Na základě konstrukce modulu UniAVV lze stanovit, že použité subsystémy mají exponenciální rozdělení pravděpodobnosti dob do poruchy. Tyto pravděpodobnosti jsou mimo jiné závislé na intervalu provádění automatických diagnostických testů a diagnostickém pokrytí modulu. Jejich hodnoty jsou tedy ovlivněny parametry λ_{DD}, λ_{DU} (intenzita nebezpečných diagnostikovaných, resp. nediagnostikovaných poruch), t_{PT} (interval automatických diagnostických testů) a t_{LT} (doba provozu modulu). Pak je možné zapsat:

$$F_{DU-I3}(t) = 1 - \exp[-(\lambda_{DD-I3} \cdot t_{PT-I3} + \lambda_{DU-I3} \cdot t_{LT-I3})] \quad [-] \tag{6.12}$$

$$F_{DU-L1}(t) = 1 - \exp[-(\lambda_{DD-L1} \cdot t_{PT-L1} + \lambda_{DU-L1} \cdot t_{LT-L1})] = F_{DU-L2}(t) \quad [-] \tag{6.13}$$

Grafický průběh pravděpodobnosti nebezpečné nediagnostikované poruchy, která charakterizuje navržený teoretický model bezporuchovosti modulu UniAVV, je zobrazen na obr. č. 6.6. Pravděpodobnost $F_{DU}(t)$ zde vyjadřuje maximální možnou hodnotu, jaké může tento ukazatel dosáhnout, pokud mají jednotlivé subsystémy modulu UniAVV vyhovět požadavkům na úroveň integrity bezpečnosti (SIL) stanovené kvalitativní analýzou rizika. Pro doplnění jsou v grafu uvedeny také průběhy pravděpodobnosti nebezpečné diagnostikované

poruchy $F_{DD}(t)$, vyjadřující maximální možnou pravděpodobnost pro dovolený rozsah diagnostického pokrytí pro dané úrovně SIL.



Obr. č. 6.6: Pravděpodobnost $F_{DU}(t)$, $F_{DD}(t)$ pro různé diagnostické pokrytí

Z uvedeného teoretického modelu bezporuchovosti modulu UniAVV vychází výpočet parametrů funkční bezpečnosti, na jejichž základě je provedeno prokázání skutečnosti, zda zařízení splňuje požadovanou úroveň integrity bezpečnosti, danou stanovenými úrovněmi SIL jednotlivých jeho subsystémů.

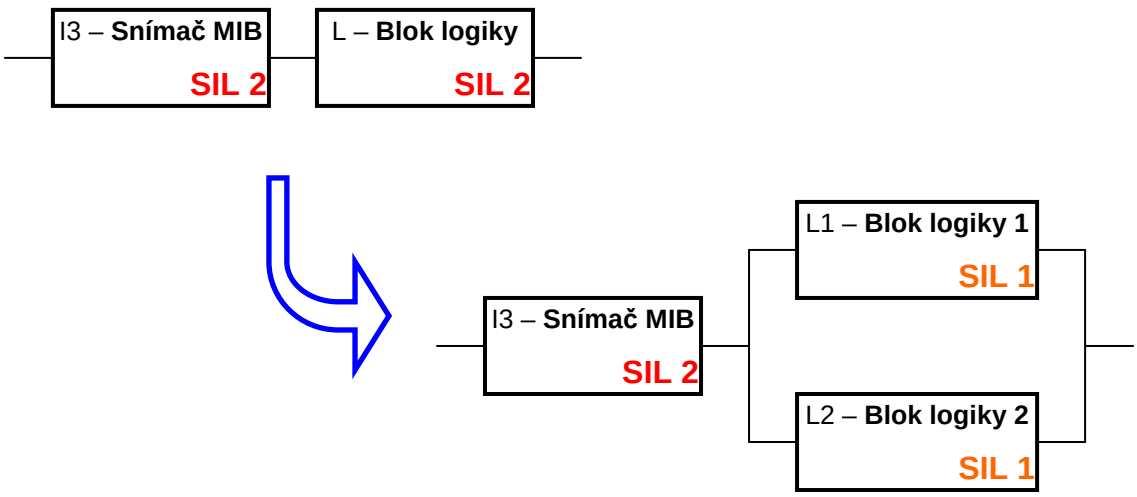
6.3 Hodnocení funkční bezpečnosti modulu UniAVV

Cílem hodnocení náhodných poruch hardware modulu UniAVV vycházejícího z principů funkční bezpečnosti je prokázání splnění požadavků daných pro jednotlivé úrovně integrity bezpečnosti (SIL). Rozhodujícími kvantitativními parametry pro důkaz dosažené bezpečnosti systému jsou cílová míra poruch a podíl bezpečných poruch (resp. diagnostické pokrytí). Určením hodnot těchto parametrů pro subsystémy modulu UniAVV je možné zjistit, zda jsou splněny požadované úrovně SIL vycházející z výsledků kvalitativní analýzy rizika modulu UniAVV.

Normami [15], [16] definované rozsahy hodnot výše uvedených parametrů, kterých má subsystém související s bezpečností dosáhnout, aby splnil požadavek na SIL, jsou závislé zejména na uspořádání architektury hardware a také na míře dostupných informací o spolehlivosti. Z tohoto důvodu je pro hodnocení spolehlivosti modulu UniAVV zvolena metoda blokových diagramů bezporuchovosti (RBD).

Z výsledků analýzy stromu poruch (FTA) vyplývá, že modul UniAVV představuje sériovou soustavu tvořenou dvěma subsystémy (subsystém logiky, subsystém signálu snímače MIB). Subsystém vstupního signálu snímače MIB představuje jednokanálové uspořádání hardware (s označením 1oo1) s odolností proti poruchám hardware $N = 0$. V tomto případě vznik nebezpečné nediagnostikované poruchy znamená ukončení schopnosti plnit požadovanou funkci. Oproti tomu blok logiky má redundantní uspořádání tvořené dvěma identickými bloky, kdy každý blok může plnit požadovanou bezpečnostní funkci. Tento subsystém tak představuje dvoukanálové uspořádání hardware (označení 1oo2) s odolností proti poruchám hardware $N = 1$. Aby subsystém nemohl plnit požadovanou bezpečnostní funkci, musí vzniknout nebezpečná nediagnostikovaná porucha obou kanálů současně.

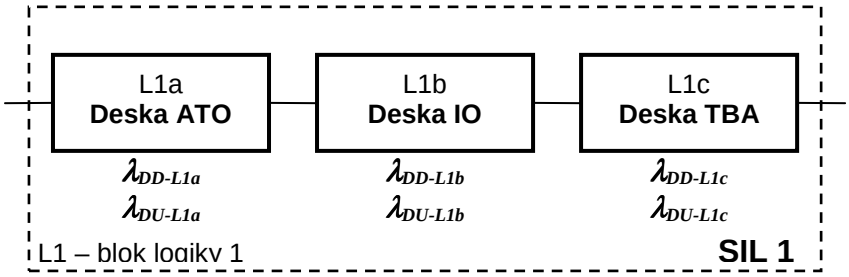
Z hodnoty parametru odolnosti proti poruchám hardware N vyplývá rozvržení požadavků SIL na jednotlivé kanály subsystémů. Z výsledků kvalitativní analýzy rizika modulu UniAVV vyplývá, že oba subsystémy by měly dosáhnout úrovně integrity bezpečnosti SIL2 pro možnost snížení rizika na přijatelnou úroveň. U subsystému tvořeného jedním kanálem musí jeho hardware tento požadavek splnit. U dvoukanálového subsystému vlivem vyšší odolnosti proti poruchám hardware se dosáhne splnění požadavku SIL2, pokud každý kanál bude splňovat úroveň SIL1, viz obr. č. 6.7.



Obr. č. 6.7: Blokové schéma modulu UniAVV s požadavky na SIL

Z hlediska konstrukčního uspořádání a charakteru informací o spolehlivosti představují uvedené dva subsystémy modulu UniAVV dva rozdílné přístupy k hodnocení jejich funkční bezpečnosti.

Kanál subsystému bloku logiky je řešen jako jeden celek zásuvného modulu do 19“ aluminiové skříně skládající se ze tří desek s plošnými spoji velkého evropského formátu s plošnými spoji a procesorovými jednotkami (viz blokové schéma na obr. č. 6.8). Jednotlivé desky jsou tvořeny běžnými elektronickými prvky (mikroprocesory, kondenzátory, rezistory, diody, tranzistory, optočleny apod.). Parametry bezporuchovosti těchto součástí (intenzity poruch) je možné zjistit přímo od jejich výrobců nebo určit výpočtem na základě standardizovaných postupů. Vzhledem ke komplexnosti uvedeného subsystému avšak nemá výrobce dostatečné informace o poruchách prvků získané z provozu zařízení, a proto je subsystém bloku logiky tvořený deskami ATO, TBA a IO klasifikován jako subsystém typu B [16].



Obr. č. 6.8: Blokové schéma bloku logiky modulu UniAVV

Naproti tomu subsystém přenosu signálu snímače MIB představuje specifický typ zařízení, tvořený samotným snímačem magnetických informačních bodů na trati (provedeným jako polarizovaný jazýčkový kontakt) a komunikačními linkami vedoucími signál do bloku logiky [23]. Výpočet v tomto případě není možný s využitím známých informací o bezporuchovosti (intenzitách poruch) tvořících prvků subsystému. Výrobce avšak disponuje věrohodnými informacemi o poruchách získaných během dostatečně dlouhé doby provozu, a proto je možné klasifikovat tento subsystém jako subsystém typu A [16], na který jsou z hlediska funkční bezpečnosti kladeny mírnější požadavky než u subsystému typu B.

Přehled informací o subsystémech modulu UniAVV a požadavcích, které musejí splnit pro prokázání požadované úrovně SIL, je uveden v tabulce č. 6.1.

Tabulka č. 6.1: Požadavky parametrů funkční bezpečnosti

Parametry, vlastnosti	Subsystém/kanál subsystému	
Subsystém	**L – blok logiky**	**I3 – snímač MIB**
Úroveň integrity bezpečnosti (SIL)	SIL2	SIL2
Typ subsystému	Subsystém typu B	Subsystém typu A
Vyžádání systému souvisejícího s bezpečností	vysoké/trvalé	vysoké/trvalé
Architektura hardware subsystému	1oo2	1oo1
Odolnost proti vadám hardware *N* [-]	1	0
Kanál subsystému	**L1 – blok logiky 1 L2 – blok logiky 2**	**I3 – snímač MIB**
Úroveň integrity bezpečnosti (SIL)	SIL1	SIL2
Poměr bezpečných poruch *SFF* [-]	**0,6 ÷ 0,9**	**0,6 ÷ 0,9**
Cílová míra poruch *PFH* [h^{-1}]	**$10^{-6} \div 10^{-5}$**	**$10^{-7} \div 10^{-6}$**

6.3.1 Určení diagnostického pokrytí

Poměr bezpečných poruch (SFF) představuje ukazatel hodnotící kvalitu diagnostického systému určeného pro detekování poruch u systémů souvisejících s bezpečností. Představuje podíl z celkového množství poruch, které byly bezpečné nebo byly diagnostikovány a tím nedošlo ke vzniku nebezpečné nediagnostikované poruchy. Analogicky je definováno diagnostické pokrytí (DC), s rozdílem, že se týká pouze nebezpečných poruch subsystémů.

Vzhledem ke skutečnosti, že při kvalitativní analýze rizika metodou diagramu rizika nebyly u modulu UniAVV klasifikovány bezpečné poruchy, je v tomto případě hodnota poměru bezpečných poruch rovna hodnotě diagnostického pokrytí (*SFF = DC*).

Hodnota diagnostického pokrytí se početně určí pro daný subsystém jako poměr intenzity nebezpečných diagnostikovaných poruch λ_{DD} k celkové intenzitě nebezpečných poruch λ_D. Pro tento případ musí být známy intenzity poruch jednotlivých tvořících prvků subsystému. V případě, že tyto údaje nejsou k dispozici, určí se hodnota diagnostického pokrytí provedením simulačního experimentu.

Pro kanál subsystému logiky (L1 nebo L2) je východiskem určení diagnostického pokrytí znalost intenzit nebezpečných poruch jeho tvořících prvků. Tento parametr je pro každý prvek tvořen dvěma složkami, jak je popsáno ve vztahu (6.14) pro blok L1:

$$\lambda_{D-L1} = \lambda_{DD-L1} + \lambda_{DU-L1} \qquad [-] \qquad (6.14)$$

kde: $\lambda_{D\text{-}L1}$ – intenzita nebezpečných poruch subsystému L1 [h^{-1}],
$\lambda_{DD\text{-}L1}$ – intenzita nebezpečných diagnostikovaných poruch subsystému L1 [h^{-1}],
$\lambda_{DU\text{-}L1}$ – intenzita nebezpečných nediagnostikovaných poruch subsystému L1 [h^{-1}].

Při předpokladu, že tvořící prvky subsystému bloku logiky mají sériové uspořádání a exponenciální rozdělení pravděpodobnosti dob do poruchy, lze určit jednotlivé složky jeho intenzity poruch jako součet odpovídajících intenzit poruch jednotlivých prvků. Viz níže vztahy pro subsystém tvořený *n* prvky:

$$\lambda_{DD-L1} = \sum_{i=1}^{n} \lambda_{DD-i} \qquad [h^{-1}] \qquad (6.15)$$

$$\lambda_{DU-L1} = \sum_{i=1}^{n} \lambda_{DU-i} \qquad [h^{-1}] \qquad (6.16)$$

Pro možnost určení jednotlivých složek intenzity poruch na úrovni tvořících prvků subsystému je nutné u jednotlivých prvků určit jejich vlastní diagnostické pokrytí DC_i. Tato hodnota je určena na základě analýzy běžných poruchových stavů, tj. přerušení obvodu (P), zkratu obvodu (Z) a změny hodnoty funkce (F). Při této analýze se zjišťuje způsob projevu poruchy a možnost její detekce diagnostickým systémem. Analýza vychází ze schémat zapojení elektronických prvků a k jejímu provedení je využit simulační nástroj OrCAD [4]. V případě, že uvedenou metodou simulace není možné určit hodnotu diagnostického pokrytí určitého prvku, použije se v souladu s normou [16] přístup, kdy se předpokládá, že 50 % poruch je zjistitelných a zbylých 50 % nikoliv. Níže uvedený vztah pro výpočet diagnostického pokrytí *i*-tého prvku DC_i zahrnuje výše uvedené způsoby poruch (P, Z, F), přičemž se předpokládá, že váha jednotlivých poruchových stavů je shodná.

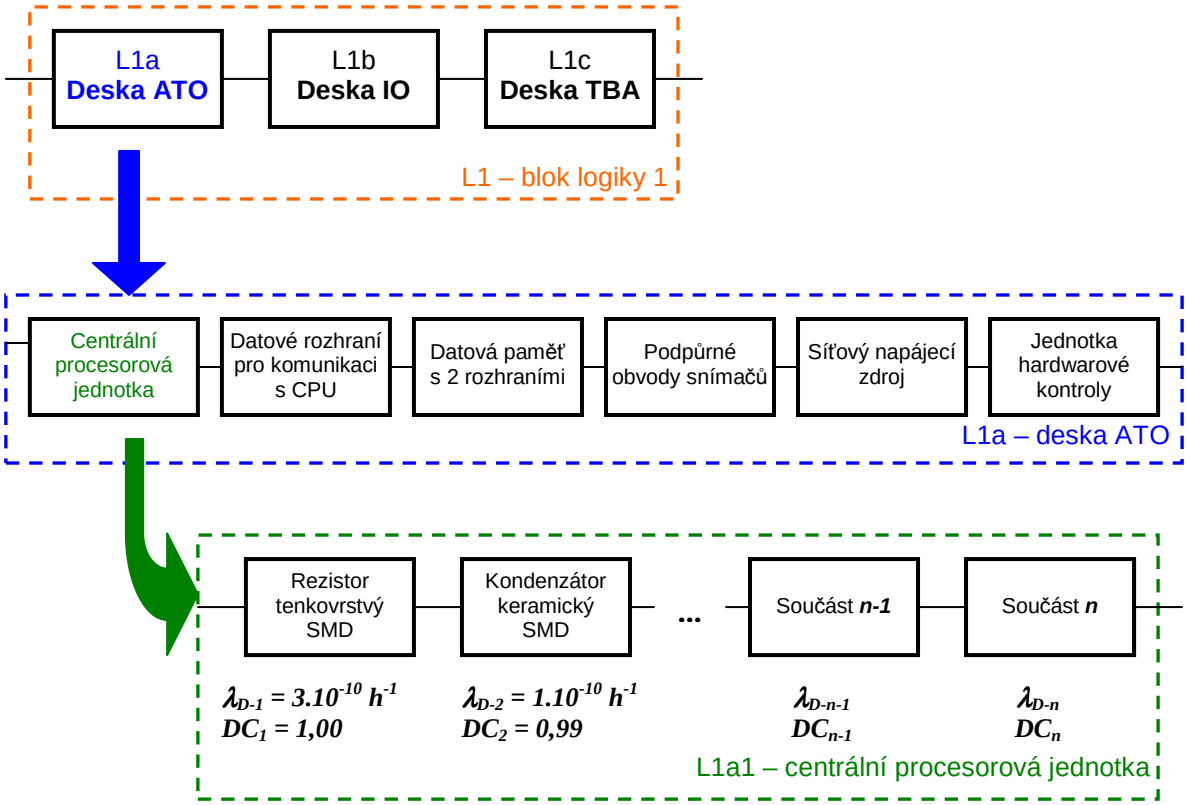
$$DC_i = \frac{1}{3} \cdot \left(DC_{i-P} + DC_{i-Z} + DC_{i-F} \right) \qquad [-] \qquad (6.17)$$

Při znalosti diagnostického pokrytí jednotlivých tvořících prvků DC_i a jejich intenzit nebezpečných poruch $\lambda_{D\text{-}i}$ je možné určit odpovídající složky intenzit poruch pro diagnostikované a nediagnostikované poruchy, neboli:

$$\lambda_{DD-i} = \lambda_{D-i} \cdot DC_i \qquad [h^{-1}] \qquad (6.18)$$

$$\lambda_{DU-i} = \lambda_{D-i} \cdot (1 - DC_i) \qquad [h^{-1}] \qquad (6.19)$$

Výpočet diagnostického pokrytí subsystému bloku logiky modulu UniAVV vychází z dekompozice jednotlivých desek na úroveň funkčních bloků a následně až na úroveň jednotlivých elektronických tvořících prvků. Fragment dekompozice desky ATO je uveden na obr. č. 6.9.



Obr. č. 6.9: Dekompozice modulu UniAVV pro určení intenzit poruch

Určení diagnostického pokrytí DC_i jednotlivých prvků je provedeno s využitím výše uvedeného postupu. Vychází z analýzy možných způsobů poruch prvků a možnosti jejich detekce. Diagnostické pokrytí prvku DC_i tak představuje pravděpodobnost, s jakou je možné diagnostikovat poruchu tohoto prvku, a zahrnuje vliv konkrétního zapojení součásti v elektrickém obvodu a mechanismy poruch, které se u ní mohou vyskytnout.

Určení intenzity nebezpečných poruch λ_{D-i} [h^{-1}] jednotlivých tvořících prvků desek bloku logiky vychází z informací o spolehlivosti od výrobců prvků. Bezporuchovost elektronických prvků je ve většině případů charakterizována intenzitou poruch. Tyto údaje

výrobci elektronických prvků uvádějí v technické dokumentaci výrobku a jsou obvykle stanoveny na základě provedení zrychlených zkoušek spolehlivosti a následného přepočtu pro předpokládanou provozní teplotu výrobku. V případě, že výrobce tyto údaje o spolehlivosti neuvádí, využije se pro jejich určení standardizovaných postupů, např. uvedených v normě „MIL HDBK 217F Military Handbook. Reliability Prediction of Electronic Equipment“, která stanovuje metodiku určení intenzit poruch elektronických prvků v závislosti na způsobu jejich použití, vlivu okolního prostředí, kvalitě provedení apod. Základní principy z této normy jsou uvedeny v příloze č. 2. Hodnoty intenzit poruch, které byly zjištěny pro jednotlivé prvky bloku logiky na základě dvou výše uvedených přístupů, jsou uvedeny v příloze č. 3.

Tabulka č. 6.2 zobrazuje výřez z výpočtu jednotlivých složek intenzit poruch prvků na základě jejich diagnostického pokrytí. Shodným postupem jsou určeny intenzity poruch všech funkčních bloků jednotlivých desek, následně desek jako celku a na závěr celého bloku logiky. Výsledky výpočtu jsou shrnuty v tabulce č. 6.3.

Tabulka č. 6.2: Diagnostické pokrytí prvku, složky intenzit poruch – výřez

Označení součástky			Přerušení obvodu		Zkratování obvodu		Změna hodnoty		$\lambda_{1souč}$ [h^{-1}]	λ_D [h^{-1}]	λ_{DD} [h^{-1}]	λ_{DU} [h^{-1}]
schématické	katalogové	počet	DD	DU	DD	DU	DD	DU				
…												
C3-4	keramicky kond. 22pF	2	1	0	1	0	1	0	1,000E-10	2,000E-10	2,000E-10	0,000E+00
Q1	Krystal 4MHz	1	1	0	1	0	0,99	0,01	4,000E-09	4,000E-09	3,987E-09	1,333E-11
C2	15pF	1	1	0	1	0	1	0	1,000E-10	1,000E-10	1,000E-10	0,000E+00
Q22	krystal 32.768 kHZ	1	1	0	1	0	0,99	0,01	4,000E-09	4,000E-09	3,987E-09	1,333E-11
R5-7	Odpor 0805, 47kΩ	3	1	0	1	0	1	0	3,000E-10	9,000E-10	9,000E-10	0,000E+00
C5	Elektrolyt 10µF/16V	1	0,99	0,01	1	0	1	0	2,000E-08	2,000E-08	1,993E-08	6,667E-11
C1	keramicky kond. 100nF	1	0,99	0,01	1	0	1	0	1,000E-10	1,000E-10	9,967E-11	3,333E-13
R58, 86	Odpor 0805, 10Ω	2	0,5	0,5	0,5	0,5	1	0	3,000E-10	6,000E-10	4,000E-10	2,000E-10
C29, 30	Tantal kond. 1µF/25V	2	0,5	0,5	0,5	0,5	1	0	1,000E-08	2,000E-08	1,333E-08	6,667E-09
…												

Při znalosti konkrétních hodnot intenzit nebezpečných diagnostikovaných a nebezpečných nediagnostikovaných poruch bloku logiky L1, resp. L2, je možné vypočítat hodnotu diagnostického pokrytí tohoto subsystému (které odpovídá hodnotě poměru bezpečných poruch):

$$DC_{L1} = \frac{\sum_{i=1}^{n} \lambda_{DD-i}}{\sum_{i=1}^{n} (\lambda_{DD-i} + \lambda_{DU-i})} = \frac{3{,}609 \cdot 10^{-5}}{3{,}609 \cdot 10^{-5} + 1{,}003 \cdot 10^{-6}} \quad [-] \qquad (6.20)$$

$$DC_{L1} = 0{,}973 \ [-] \qquad (6.21)$$

Uvedený výsledek diagnostického pokrytí D_{CL1} lze interpretovat tak, že s pravděpodobností 97,3 % bude vzniklá nebezpečná porucha subsystému bloku logiky zjištěna a systém související s bezpečností aktivuje bezpečnostní funkci, čímž uvede modul UniAVV do bezpečného stavu.

Pro druhý subsystém modulu UniAVV, tj. subsystému přenosu signálu snímače MIB, je jeho diagnostické pokrytí DC_{I3} určeno na základě simulačního experimentu, kdy je vyhodnocována možnost detekce jeho poruch. Pro tento subsystém je určena hodnota diagnostického pokrytí na úrovni 99 %.

Tabulka č. 6.3: Intenzity poruch, poměr bezpečných poruch bloku logiky

Deska ATO	**λ_D [h^{-1}]**	**λ_{DD} [h^{-1}]**	**λ_{DU} [h^{-1}]**
Centrální procesorová jednotka	2,905E-07	2,824E-07	8,185E-09
Datová rozhraní pro přímou komunikaci s CPU	6,224E-06	6,218E-06	6,224E-09
Jednotka datové paměti s 2 rozhraními	5,411E-07	5,406E-07	5,040E-10
Podpůrné obvody snímačů	2,180E-06	2,121E-06	5,851E-08
Síťový napájecí zdroj	1,463E-06	1,327E-06	1,365E-07
Jednotka hardwarové kontroly proti "zbloudění" programu	1,260E-07	1,146E-07	1,138E-08
Deska celkem	**1,083E-05**	**1,060E-05**	**2,213E-07**
Deska TBA	**λ_D [h^{-1}]**	**λ_{DD} [h^{-1}]**	**λ_{DU} [h^{-1}]**
Centrální procesorová jednotka a podpůrné obvody	3,130E-07	3,006E-07	1,240E-08
Datová rozhraní pro komunikaci s CPU	9,315E-06	9,306E-06	9,315E-09
Jednotka datové paměti s 2 rozhraními	5,411E-07	5,406E-07	5,040E-10
Síťový napájecí zdroj	7,547E-07	7,512E-07	3,388E-09
Deska celkem	**1,092E-05**	**1,090E-05**	**2,560E-08**
Deska IO	**λ_D [h^{-1}]**	**λ_{DD} [h^{-1}]**	**λ_{DU} [h^{-1}]**
2 x 2 magnetické snímače	6,890E-06	6,820E-06	6,890E-08
Blok diagnostiky magnetických snímačů	1,294E-06	1,281E-06	1,294E-08
Obvod návěstní opakovač	1,130E-06	5,781E-07	5,515E-07
Spínač brzdového ventilu se 2 výstupy	7,340E-07	7,266E-07	7,340E-09
7 x Spínač brzdového ventilu	4,607E-06	4,561E-06	4,607E-08
Pom. mikrokontrolér a obvody interního datového rozhraní	1,533E-07	1,513E-07	1,982E-09
Blok Master/slave	2,706E-07	2,679E-07	2,706E-09
Jednotka hardwarové kontroly proti "zbloudění" programu	2,703E-07	2,0554E-07	6,4799E-08
Deska celkem	**1,535E-05**	**1,459E-05**	**7,562E-07**
Jednotka logiky celkem	**λ_D [h^{-1}]**	**λ_{DD} [h^{-1}]**	**λ_{DU} [h^{-1}]**
Intenzita poruch	**3,710E-05**	**3,609E-05**	**1,003E-06**
Poměr bezpečných poruch *SFF* [-]:	**0,973**		

6.3.2 Určení cílové míry poruch

Pro modul UniAVV, který je klasifikován jako systém související s bezpečností pracující v režimu provozu s vysokým nebo trvalým vyžádáním bezpečnostní funkce, je cílová míra poruch *PFH* definována jako pravděpodobnost nebezpečných poruch *PFD* vztažená na jednotku času [17]. Nebezpečná porucha systému z pohledu funkční bezpečnosti představuje poruchu, kterou není možné detekovat. Jedná se tedy o nebezpečnou nediagnostikovanou poruchu, jejíž pravděpodobnost $F_{DU}(t)$ je možné určit s využitím vztahu odvozeného z teoretického modelu spolehlivosti modulu UniAVV. Tedy platí:

$$F_{DU}(t) = PFD \qquad [-] \tag{6.22}$$

Doba provozu modulu UniAVV, pro kterou je cílová míra poruch určována, je stanovena jako předpokládaná doba životnosti zařízení, která je uvedena výrobcem v technické dokumentaci. Tento přístup je zvolen z důvodu tzv. účinku nedokonalé kontrolní (periodické) zkoušky [19], kdy některé poruchy systému souvisejícího s bezpečností nemohou být zjištěny vlivem nedokonalého diagnostického systému až do vyžádání bezpečnostní funkce, případně po celou dobu životnosti systému.

Hodnota cílové míry poruch *PFH* jednotlivých subsystémů modulu UniAVV je závislá na hodnotách faktorů, které ji ovlivňují. Patří mezi ně:

- intenzita nebezpečných nediagnostikovaných a diagnostikovaných poruch λ_{DU}, resp. λ_{DD} určená na základě dříve provedeného výpočtu diagnostického pokrytí *DC*,
- životnost modulu UniAVV, která je stanovena jako akumulovaná doba provozu zařízení (bez uvážení prostojů, doby údržby a oprav) a její hodnota stanovená výrobcem je t_{LT} = 50 000 hodin,
- interval provádění automatických diagnostických testů t_{PT}; u některých částí zařízení jsou diagnostické testy prováděny kontinuálně (např. hardwarová ochrana procesorů typu watch-dog), u některých částí zařízení jsou diagnostické testy prováděny pouze při aktivaci systému řízení lokomotivy; hodnota intervalu těchto testů je zvolena t_{PT} = 12 hodin, jako maximální doba mezi aktivacemi systému řízení vozidla s ohledem na střídání lokomotivních čet.

Výpočet cílové míry poruch *PFH* se provede pro oba subsystémy modulu UniAVV s cílem prokázat, zda hodnota tohoto ukazatele funkční bezpečnosti splňuje kritéria daná pro požadovanou úroveň integrity bezpečnosti (SIL).

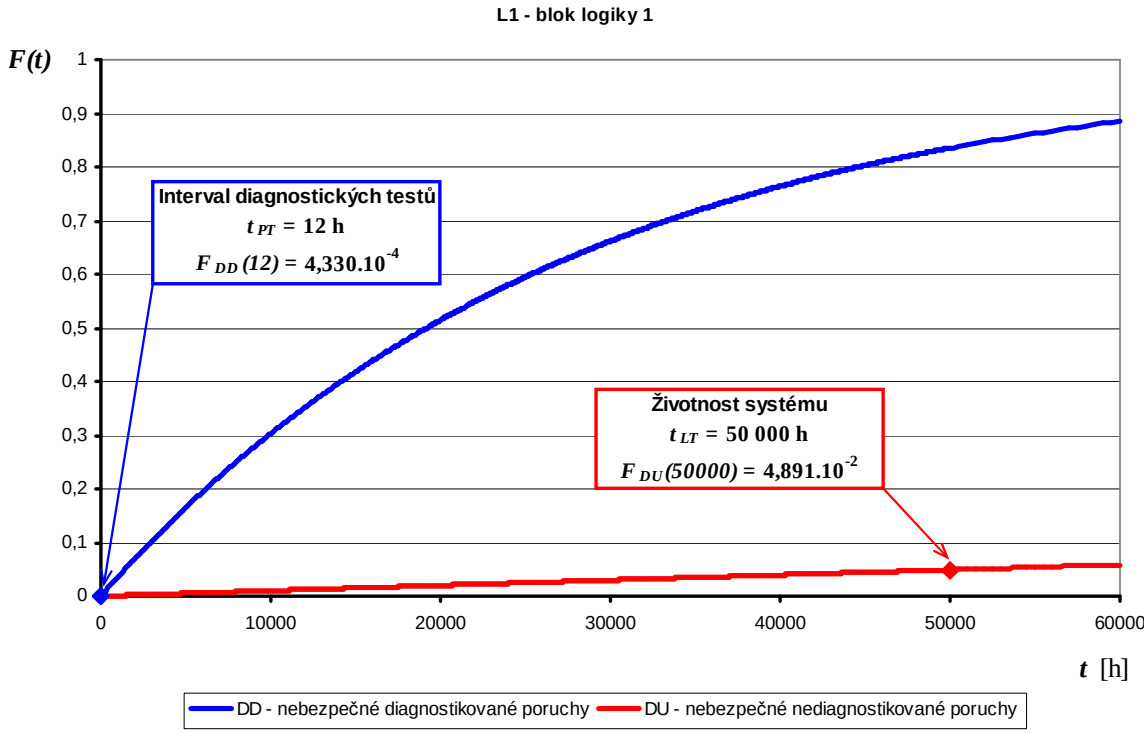
Pro subsystém bloku logiky L1 (nebo identicky pro L2) se nejdříve určí pravděpodobnost nebezpečné nediagnostikované poruchy PFD_{L1} s využitím vztahu (6.13), neboli:

$$PFD_{L1} = 1 - \exp\left[-\left(\lambda_{DD-L1} \cdot t_{PT-L1} + \lambda_{DU-L1} \cdot t_{LT-L1}\right)\right] \quad [-] \tag{6.23}$$

$$PFD_{L1} = 1 - \exp\left[-\left(3{,}609 \cdot 10^{-5} \cdot 12 + 1{,}003 \cdot 10^{-6} \cdot 50000\right)\right] \quad [-] \tag{6.24}$$

$$PFD_{L1} = 4{,}933 \cdot 10^{-2} \ [-] \tag{6.25}$$

Grafické znázornění vypočtených složek pravděpodobnosti PFD_{L1} je zobrazeno v grafu představujícím průběh pravděpodobnosti diagnostikované a nediagnostikované poruchy po dobu životnosti modulu UniAVV, viz obr. č. 6.10.



Obr. č. 6.10: Blok logiky, pravděpodobnost poruchy $F_{DD}(t)$, $F_{DU}(t)$

Následně je možné provést výpočet hodnoty cílové míry poruch PFH_{L1} dosazením do vztahu (3.9):

$$PFH_{L1} = \frac{PFD}{t_{LT}} = \frac{4{,}933 \cdot 10^{-2}}{50000} \quad [h^{-1}] \tag{6.26}$$

$$PFH_{L1} = 9{,}865 \cdot 10^{-7} \ [h^{-1}] \tag{6.27}$$

Pro možnost určení hodnoty cílové míry poruch subsystému přenosu signálu snímače MIB je nutné nejdříve zjistit hodnotu intenzity nebezpečných poruch $\lambda_{D\text{-}I3}$. Na základě výše uvedené charakteristiky subsystému je tato hodnota vypočtena na základě údajů o spolehlivosti získaných z provozu zařízení. Při splnění požadavků norem funkční bezpečnosti ČSN EN 61508 na dobu provozu minimálně jeden rok a věrohodnost informací s konfidenční úrovní minimálně 70 %, má intenzita nebezpečných poruch $\lambda_{D\text{-}I3}$ hodnotu:

$$\lambda_{D-I3} = 8{,}44 \cdot 10^{-6} \ [\text{h}^{-1}] \tag{6.28}$$

Podrobný postup výpočtu této hodnoty z dat získaných provedením zkoušky spolehlivosti je uveden v kapitole č. 7.1.

Dále jsou s využitím známé hodnoty diagnostického pokrytí DC_{I3} určeny pro subsystém přenosu signálu snímače MIB jednotlivé složky intenzity poruch, tedy intenzita nebezpečných diagnostikovaných poruch, $\lambda_{DD\text{-}I3} = 8{,}36.10^{-6}$ [h^{-1}], a také intenzita nebezpečných nediagnostikovaných poruch, $\lambda_{DU\text{-}I3} = 8{,}44.10^{-8}$ [h^{-1}]. Na jejich základě může být vypočtena hodnota intenzity nebezpečných nediagnostikovaných poruch PFD_{I3} a hodnota cílové míry poruch PFH_{I3}, které se určí analogicky jako u subsystému bloku logiky.

$$PFD_{I3} = 1 - \exp\left[-\left(8{,}36 \cdot 10^{-6} \cdot 12 + 8{,}44 \cdot 10^{-8} \cdot 50000\right)\right] \quad [\text{-}] \tag{6.29}$$

$$PFD_{I3} = 4{,}31 \cdot 10^{-3} \ [\text{-}] \tag{6.30}$$

$$PFH_{I3} = \frac{PFD}{t_{LT}} = \frac{4{,}31 \cdot 10^{-3}}{50000} \quad [\text{h}^{-1}] \tag{6.31}$$

$$PFH_{I3} = 8{,}62 \cdot 10^{-8} \ [\text{h}^{-1}] \tag{6.32}$$

6.3.3 Zhodnocení dosažených výsledků

Cílem výpočtu ukazatelů funkční bezpečnosti je prokázání splnění kritérií daných pro požadovanou úroveň integrity bezpečnosti (SIL) u jednotlivých subsystémů souvisejících s bezpečností z hlediska náhodných poruch hardware. Srovnání dosažených výsledků u subsystémů modulu UniAVV s požadavky danými normou ČSN EN 61508 je uvedeno v tabulce č. 6.4.

Tabulka č. 6.4: Porovnání dosažených výsledků

Parametr	Označení		L1 Blok logiky 1	I3 Snímač MIB
Požadavky				
Úroveň integrity bezpečnosti	*SIL*		SIL1	SIL2
Diagnostické pokrytí	*DC*	[-]	0,6 ÷ 0,9	0,6 ÷ 0,9
Cílová míra poruch	*PFH*	[h^{-1}]	$10^{-6} \div 10^{-5}$	$10^{-7} \div 10^{-6}$
Vypočtené výsledky				
Intenzita nebezpečných poruch	λ_D	[h^{-1}]	$3{,}710.10^{-5}$	$8{,}44.10^{-6}$
Intenzita nebezpečných diagnostikovaných poruch	λ_{DD}	[h^{-1}]	$3{,}609.10^{-5}$	$8{,}356.10^{-6}$
Intenzita nebezpečných nediagnostikovaných poruch	λ_{DU}	[h^{-1}]	$1{,}003.10^{-6}$	$8{,}44.10^{-8}$
Diagnostické pokrytí	*DC*	[-]	**0,973**	**0,99**
Interval automatických diagnostických testů	t_{PT}	[h]	12	12
Doba životnosti systému	t_{LT}	[h]	50 000	50 000
Pravděpodobnost nebezpečných poruch	*PFD*	[-]	$4{,}933.10^{-2}$	$4{,}31.10^{-3}$
Cílová míra poruch	*PFH*	[h^{-1}]	**$9{,}865.10^{-7}$**	**$8{,}62.10^{-8}$**

Vypočtené hodnoty ukazatelů funkční bezpečnosti pro hodnocení náhodných poruch hardware systémů souvisejících s bezpečností, tedy diagnostické pokrytí (DC) a cílová míra poruch (PFH), u modulu UniAVV vyhověly požadavkům pro stanovenou úroveň integrity bezpečnosti, tedy SIL1 u subsystému bloku logiky a SIL2 u subsystému snímače MIB.

Hodnota diagnostického pokrytí (DC) je jak u subsystému bloku logiky, tak také subsystému snímače MIB vyšší, než je rozmezí stanovené pro požadovanou úroveň integrity bezpečnosti. Z hlediska kvality a účinnosti diagnostického systému tak subsystémy modulu UniAVV vyhovují vyšší úrovni SIL, než jaká je pro ně požadována v souvislosti s potřebnou redukcí rizika na přípustnou úroveň.

Hodnota cílové míry poruch (PFH), hodnotící úroveň bezporuchovosti systémů souvisejících s bezpečností, je u obou subsystémů modulu UniAVV nižší, než je normou stanovené rozmezí pro požadovanou úroveň SIL. Vyšší než požadovaná úroveň integrity bezpečnosti (SIL) nebude u subsystémů modulu UniAVV deklarována. Jedním z důvodů tohoto přístupu je skutečnost, že s vyšší hodnotou SIL hardware by došlo také ke zvýšení požadavků na jeho architekturu a nutnosti aplikace nových opatření také pro funkční bezpečnost software nad rámec opatření nutných ke snížení rizika na přípustnou úroveň.

Z hlediska uspořádání architektury hardware subsystém bloku logiky, který má dvoukanálové uspořádání (1oo2), kdy je zajištěna odolnost proti poruchám hardware $N = 1$, splňuje požadavek na SIL2, když je prokázáno, že jednotlivé kanály vyhovují úrovni integrity bezpečnosti SIL1. Subsystém snímače MIB představuje jednokanálové uspořádání architektury hardware (1oo1), u kterého je prokázána úroveň integrity bezpečnosti SIL2.

Vzhledem k požadované úrovni integrity bezpečnosti SIL2 pro oba subsystémy modulu UniAVV není nutné dle normy ČSN EN 61508 hodnotit funkční bezpečnost hardware z pohledu systematických poruch, které u něho mohou vyskytovat.

Pro úplné zhodnocení funkční bezpečnosti E/E/PE systémů souvisejících s bezpečností je nutné pro požadovanou úroveň integrity bezpečnosti (SIL) mimo hodnocení hardware provést také hodnocení software. Tato problematika ovšem nespadá do zaměření této práce, a proto zde není více zmiňována.

7 NÁVRH PROGRAMU ZKOUŠEK SPOLEHLIVOSTI PRO MODUL UniAVV

Spolehlivost představuje zásadní vlastnost technických systémů, která má značný vliv na jejich celkovou kvalitu a bezpečnost. Odběratelé těchto výrobků obvykle požadují objektivní informace o jejich skutečné dosažené spolehlivosti. V zájmu zachování konkurenceschopnosti je tedy žádoucí, aby výrobci u svých výrobků prokázali a ověřili reálnou úroveň požadovaných parametrů spolehlivosti. To platí také pro modul automatického vedení vlaku UniAVV, který je součástí komplexního systému kolejového vozidla, jehož činnost ovlivňuje bezpečnost provozu železniční dopravy.

Určení skutečné úrovně bezporuchovosti systému, která ve značné míře ovlivňuje také jeho bezpečnost, je vhodné provést realizací zkoušek spolehlivosti. Na základě testování omezeného počtu výrobků lze použitím nástrojů matematické statistiky určit nebo ověřit hodnoty konkrétních parametrů bezporuchovosti, které je možné s vysokou věrohodností vztáhnout na celou populaci daného výrobku.

Cílem prováděných zkoušek spolehlivosti je získat požadované informace v nejkratším možném čase, přičemž je zachována jejich dostatečná věrohodnost. Z tohoto důvodu zkoušky spolehlivosti obvykle probíhají v laboratorních podmínkách, kdy jsou zkoušené výrobky podrobeny zvýšenému zatížení. Efektivních výsledků z hlediska časové náročnosti lze avšak dosáhnout také prováděním zkoušek spolehlivosti v provozních podmínkách výrobku. V tomto případě pro urychlení zkoušky lze využít informací o provozní spolehlivosti konstrukčně shodných systémů předešlých generací.

Pro možnost objektivního a snadného vyhodnocení výsledků zkoušek spolehlivosti je nutné pro každou realizovanou zkoušku zajistit konkrétní program jejího provádění. V něm je potřeba stanovit postup zkoušky, definovat podmínky a určit její parametry. Na základě těchto informací je stanovena metodika výpočtu požadovaných parametrů spolehlivosti a navrženy účinné nástroje pro možnost vyhodnocení zkoušky.

7.1 Provozní zkouška spolehlivosti snímače MIB

Při hodnocení náhodných poruch hardware E/E/PE subsystémů souvisejících s bezpečností je nutné v souladu s principy funkční bezpečnosti prokázat dosaženou úroveň

integrity bezpečnosti (SIL). Toto hodnocení se provádí na základě odhadu intenzity nebezpečných poruch subsystému. V případě, že tuto hodnotu nelze určit analytickým přístupem, který vyžaduje znalost intenzit poruch jednotlivých tvořících prvků subsystému, je nutné intenzitu nebezpečných poruch určit provedením zkoušky spolehlivosti. Jak vyplývá z kvantitativního hodnocení spolehlivosti modulu UniAVV, pro subsystém přenosu signálu snímače MIB není možné určit intenzitu nebezpečných poruch s využitím teoretického modelu bezporuchovosti vzhledem ke specifičnosti konstrukce tohoto zařízení.

Z výše uvedeného důvodu je tedy nutné pro zjištění hodnoty intenzity nebezpečných poruch tohoto subsystému využít informací o spolehlivosti získaných z provozu zařízení. V situaci, kdy subsystém je ve stádiu vývoje a nejsou k dispozici údaje o jeho skutečné provozní spolehlivosti, je možné dle principů funkční bezpečnosti použít data z předchozího provozu systému v obdobném typu prostředí. Podle normy [16] se pro dostatečně věrohodný a průkazný odhad intenzity poruch požaduje splnění následujících podmínek:

- konfidenční úroveň *C* pro dolní mez jednostranného odhadu intenzity poruch má dosahovat minimálně hodnoty 70 %,
- provozní doba jednotlivých zařízení, jejichž údaje o bezporuchovosti jsou využívány pro odhad intenzit poruch, musí být delší než jeden rok,
- předchozí provoz subsystému probíhá ve stejných nebo dostatečně blízkých podmínkách, v nichž bude provozován subsystém v současném řešení,
- do provozní doby zařízení je zahrnuta pouze ta část, kdy jsou důsledně zaznamenávány údaje o bezporuchovosti zařízení, tj. o vzniku poruch (kategorie, příčiny apod.).

Shodná konstrukce snímače MIB, který je součástí modulu UniAVV u lokomotivy 109E (řada 380 ČD), je použita také u snímače MIB elektrické jednotky řady 471 ČD. Vzhledem ke skutečnosti, že snímače MIB u obou typů vozidel plní shodné funkce, tj. identifikace polohy vozidla na trati čtením informací traťových magnetických informačních bodů (MIB), a jsou umístěny na vozidlech ve shodné poloze, lze předpokládat, že jejich provoz probíhá ve shodných podmínkách.

Provozovatel elektrických jednotek řady 471, České dráhy, a.s., zaznamenává informace o provozní spolehlivosti jednotlivých subsystémů vozidla, včetně snímačů MIB. Určení požadovaných parametrů bezporuchovosti v souladu s principy funkční bezpečnosti vychází z evidence nebezpečných poruch. Nebezpečná porucha snímače MIB je definovaná

jako chybné přečtení kódu magnetického informačního bodu na trati. To může vést ke vzniku nebezpečné události, kdy modul UniAVV předpokládá jinou polohu vozidla, než kde se ve skutečnosti nachází.

Pro možnost vyhodnocení parametrů bezporuchovosti z pohledu funkční bezpečnosti byly provozovatelem vozidel poskytnuty údaje o dvanácti snímačích MIB, umístěných na třech elektrických jednotkách řady 471. Po dobu provozu delší než jeden rok nevznikla u sledovaných snímačů MIB žádná nebezpečná porucha, viz prohlášení Českých drah, a.s. v příloze č. 4. Provozní doba jednotlivých snímačů MIB ve sledovaném období je uvedena v tabulce č. 7.1.

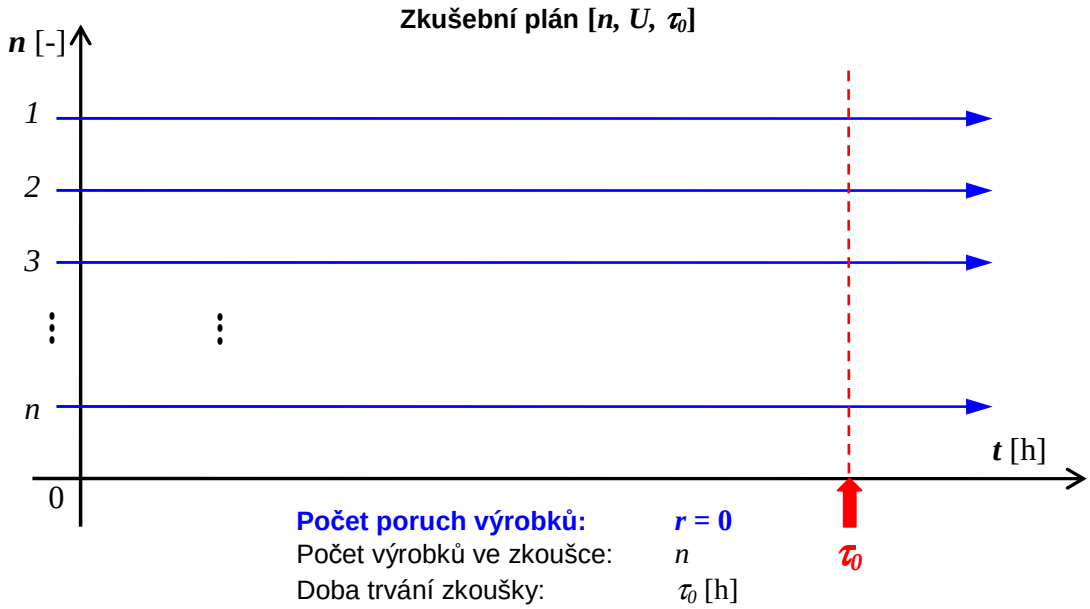
Tabulka č. 7.1: Snímače MIB, akumulovaná pracovní doba zkoušky

č. jednotky	Začátek zkoušky	Konec zkoušky	počet snímačů	t_{AKU} vozidla [h]
39	26.3.2008	19.11.2009	4	57888
41	29.7.2008	19.11.2009	4	45984
43	13.10.2008	19.11.2009	4	38784

Uvedený případ odhadu intenzity nebezpečných poruch vycházející z informací o bezporuchovosti subsystému přenosu signálu snímače MIB lze považovat z pohledu zkoušek spolehlivosti za specifickou zkoušku prováděnou podle *t*-plánu (viz schéma zkoušky uvedené na obr. č. 7.1). Jejím cílem je určit hodnotu dosud neznámého parametru rozdělení pravděpodobnosti dob do poruchy.

Tento zkušební plán s označením [n, U, τ] představuje zkoušku, do které je zařazeno n shodných výrobků a doba jejího trvání je τ [h]. Jak vyplývá z údajů o provozní spolehlivosti provozovatele elektrických jednotek řady 471, během doby zkoušky u snímačů MIB nedošlo k žádné nebezpečné poruše. Získané doby provozu jednotlivých snímačů tedy nejsou určeny vznikem poruchy, ale dobou trvání zkoušky. Získaná data jsou tedy cenzurovaná a představují jednoduše cenzurovaný soubor II. typu. Není možné tomuto souboru dat přiřadit konkrétní průběh rozdělení pravděpodobnosti náhodné veličiny, například exponenciální rozdělení, které se u snímače MIB předpokládá z důvodu charakteru jeho konstrukce. Proto není možné pro intervalový odhad intenzity nebezpečných poruch λ_D [h^{-1}] využít například metodu věrohodnostního poměru, popsanou v [20], která je určena pouze pro necenzurované soubory dat.

Pro odhad neznámé hodnoty parametru bezporuchovosti u uvedeného zkušebního plánu je vhodné využít výpočtu založeného na použití chí-kvadrát statistiky pro určitý počet stupňů volnosti 2ν a požadovanou konfidenční úroveň C.



Obr. č. 7.1: Schéma zkušebního t-plánu pro $r = 0$ poruch

Počet stupňů volnosti statistiky chí-kvadrát 2ν je závislý na počtu poruch r, které vzniknou u výrobků zařazených do zkoušky. Pro uvedený případ zkoušky, kdy během jejího trvání nevznikne žádná porucha, platí:

$$2\nu = 2 \cdot (r+1) = 2 \cdot (0+1) = 2 \qquad [-] \qquad (7.1)$$

Akumulovaná pracovní doba zkoušky t_{AKU} představuje součet všech dob činnosti všech výrobků zařazených do zkoušky. Obecně pro uvedený zkušební plán platí:

$$t_{AKU} = n \cdot \tau_0 \qquad [\text{h}] \qquad (7.2)$$

Tento přístup je možný pouze v případě, kdy zkouška u všech výrobků začíná a končí ve stejném okamžiku, což je obvyklé pouze v laboratorních podmínkách. V technické praxi, kdy zkouška probíhá během běžného provozu, toto není možné dosáhnout. Doba provozu sledovaných zařízení je ovlivněna různými okamžiky zahájení provozu, vznikem provozních prostojů apod. Pro akumulovanou pracovní dobu zkoušky platí, že je dána součtem jednotlivých dílčích dob provozu zkoušených výrobků, tedy:

$$t_{AKU} = \sum_{i=1}^{n} \tau_{0i} \quad [\text{h}] \tag{7.3}$$

S využitím výše uvedených charakteristik lze vypočítat intervalový odhad parametru rozdělení pravděpodobnosti doby do poruchy, kterým může být např. střední doba do poruchy *E(T)* [h]. Dolní mez jednostranného intervalu střední doby do poruchy T_D pro požadovanou minimální konfidenční úroveň $C = 0{,}7$ je možné určit:

$$T_D \geq \frac{2 \cdot t_{AKU}}{\chi^2_{2;0,7}} \quad [\text{h}] \tag{7.4}$$

kde: T_D – dolní mez intervalového odhadu střední doby do poruchy [h],
t_{AKU} – akumulovaná pracovní doba výrobků ve zkoušce [h],
$\chi^2_{2;0,7}$ – hodnota statistiky chí-kvadrát [-], pro počet stupňů volnosti $2\nu = 2$ a konfidenční úroveň $C = 0{,}7$.

Po dosazení konkrétní hodnoty chí-kvadrát statistiky lze vztah (7.4) převést na jednoduchou funkci, která je závislostí pouze doby provozu jednotlivých zařízení zařazených do zkoušky:

$$T_D \geq \frac{2 \cdot t_{AKU}}{2{,}408} = 0{,}831 \cdot \sum_{i=1}^{n} \tau_{0i} \quad [\text{h}] \tag{7.5}$$

Dolní odhad požadovaného parametru, tj. intenzity nebezpečných poruch subsystému souvisejícího s bezpečností λ_D [h^{-1}], je možné určit převodním vztahem mezi střední hodnotou a intenzitou poruch pro exponenciální rozdělení. Toto rozdělení lze předpokládat pro necenzurované soubory dat z důvodu charakteru konstrukce zařízení (elektrotechnický systém). Pak platí:

$$\lambda_D \leq \frac{1}{T_D} \quad [\text{h}^{-1}] \tag{7.6}$$

Pro zkoušku spolehlivosti snímačů MIB jsou k dispozici provozní údaje o spolehlivosti ze tří elektrických jednotek řady 471. Do zkoušky je tedy zařazeno 12 snímačů MIB, přičemž u každého z nich byla doba provozu (doba trvání zkoušky) delší než jeden rok, viz výše tabulka č. 7.1. Akumulovaná pracovní doba zkoušky činila:

$$t_{AKU} = \sum_{i=1}^{12} \tau_{0i} = 142\ 656\ [\text{h}] \tag{7.7}$$

Dosazením této hodnoty do vztahu (7.5) lze získat dolní mez jednostranného intervalového odhadu střední doby do poruchy T_D [h] pro požadovanou minimální konfidenční úroveň $C = 0{,}7$.

$$T_D \geq 0{,}831 \cdot 142\ 656 \qquad [\text{h}] \tag{7.8}$$

$$T_D \geq 118\ 488\ [\text{h}] \tag{7.9}$$

Tato hodnota charakterizuje parametr provozní spolehlivosti celé populace výrobků (všech provozovaných snímačů MIB). S pravděpodobností 70 % je střední doba do nebezpečné poruchy snímače MIB rovna nebo vyšší než je tato vypočtená hodnota.

Požadovaná hodnota intenzity nebezpečných poruch λ_D [h^{-1}] daná jako jednostranný intervalový odhad se určí:

$$\lambda_D \leq \frac{1}{118\ 488} \qquad [\text{h}^{-1}] \tag{7.10}$$

$$\lambda_D \leq 8{,}44 \cdot 10^{-6}\ [\text{h}^{-1}] \tag{7.11}$$

Vypočtená hodnota intenzity nebezpečných poruch subsystému přenosu signálu snímače MIB, získaná provedením určovací zkoušky spolehlivosti z informací získaných z provozu zařízení, je následně použita při hodnocení funkční bezpečnosti pro prokázání dosažené úrovně integrity bezpečnosti (SIL).

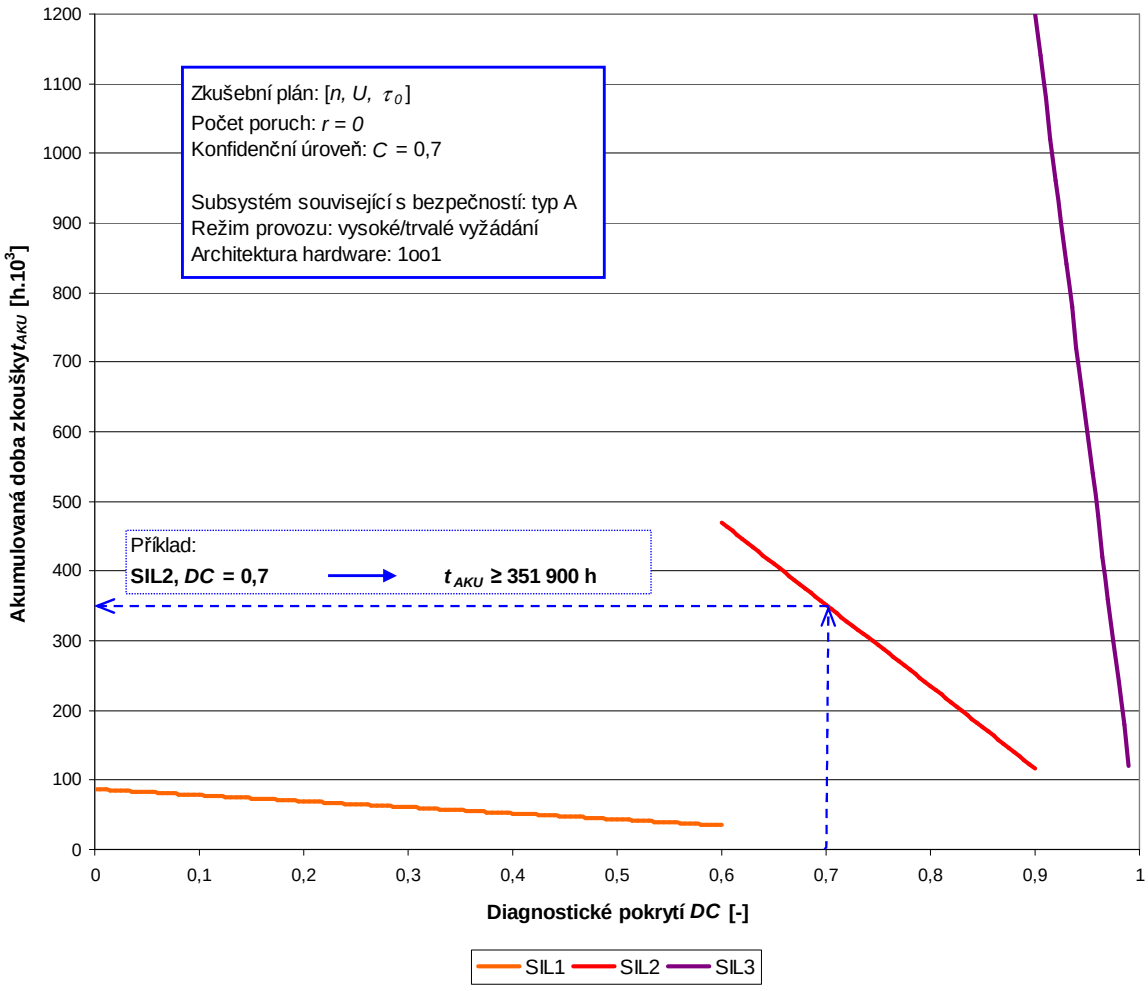
Ve spojení určující zkoušky spolehlivosti s principy funkční bezpečnosti přechází uvedená zkouška spolehlivosti do formy „kombinované“ zkoušky. Tato zkouška spojuje principy zkoušky určující pro určení intenzity nebezpečných poruch subsystému a zkoušky ověřovací, jejímž cílem je ověření (prokázání) dosažené úrovně SIL.

Princip této zkoušky spolehlivosti je založen na výše provedené zkoušce, vycházející z provozních dat o spolehlivosti a předpokladu, že během ní nevznikly žádné poruchy. Cílem tohoto přístupu je stanovit, jak dlouho musí zkouška spolehlivosti probíhat, aby mohla být prokázána požadovaná úroveň SIL.

Konkrétním výsledkem uvedeného přístupu je určení minimální požadované akumulované pracovní doby zkoušky t_{AKU} [h], tj. součtu doby provozu jednotlivých výrobků zařazených do zkoušky, přičemž během zkoušky u žádného výrobku nesmí dojít ke vzniku nebezpečné poruchy. Tato hodnota je určena pro požadovanou konfidenční úroveň $C = 0{,}7$,

maximální dovolenou cílovou míru poruch *PFH* pro danou úroveň SIL a úroveň diagnostického pokrytí *DC*, kterou dosahuje zkoušený subsystém související s bezpečností.

Grafické vyjádření závislosti akumulované pracovní doby zkoušky na dosaženém diagnostickém pokrytí subsystému souvisejícího s bezpečností, tedy funkce $t_{AKU} = f(DC)$, pro úrovně integrity bezpečnosti SIL1, SIL2 a SIL3 za výše uvedených podmínek, je uvedeno na obr. č. 7.2. V uvedeném příkladu je rozsah diagnostického pokrytí určen pro subsystémy související s bezpečností typu A (jsou k dispozici dostatečně věrohodné údaje o provozní spolehlivosti zařízení) s architekturou hardware 1oo1 (jednokanálové uspořádání) a cílovou míru poruch pro subsystémy pracující v režimu s vysokým nebo trvalým vyžádáním bezpečnostní funkce (odpovídá subsystému přenosu signálu snímače MIB).



Obr. č. 7.2: Akumulovaná doba zkoušky pro prokázání SIL v závislosti na DC

Výše uvedený přístup lze demonstrovat na příkladu pro subsystém modulu UniAVV, tj. snímač MIB. Pro požadavek na úroveň integrity bezpečnosti SIL2 a zjištěné diagnostické

pokrytí $DC = 0{,}99$ (překračující požadovanou úroveň pro SIL2) je z odpovídajícího průběhu závislosti $t_{AKU} = f(DC)$ (mimo zobrazený rozsah výše uvedeného grafu) určeno, že pro splnění uvedených požadavků musí akumulovaná pracovní doba výrobků ve zkoušce spolehlivosti na hladině významnosti $C = 0{,}7$ činit minimálně 11 730 hodin, aniž by vznikla porucha kteréhokoliv zkoušeného výrobku. Při reálném provedení zkoušky spolehlivosti pro subsystém snímače MIB byla zaznamenána akumulovaná pracovní doba $t_{AKU} = 142\,656$ [h], která je mnohem vyšší než minimální požadovaná hodnota, a proto tento subsystém z hlediska náhodných poruch hardware splňuje požadavky na SIL2. Při tomto způsobu hodnocení, vycházejícím z provozních informací o spolehlivosti, nesmí být opomenuta skutečnost, že doba provozu každého výrobku ve zkoušce musí být delší než jeden rok.

Zobecněním uvedeného přístupu lze odvodit vztah pro minimální akumulovanou pracovní dobu zkoušky podle zkušebního plánu [n, U, τ_0] pro libovolnou konfidenční úroveň C a různý počet poruch r, které během zkoušky vzniknou, tedy:

$$t_{AKU} \geq \frac{\chi^2_{2\nu;\,C} \cdot (1 - DC)}{2 \cdot \lambda_{DU\,\max}} \quad \text{[h]} \tag{7.12}$$

kde: t_{AKU} – akumulovaná pracovní doba výrobků ve zkoušce [h],
DC – diagnostické pokrytí subsystému souvisejícího s bezpečností [-],
λ_{DUmax} – maximální intenzita nebezpečných nediagnostikovaných poruch pro požadovaný SIL [h^{-1}]
$\chi^2_{2\nu;C}$ – hodnota statistiky chí-kvadrát [-], pro počet stupňů volnosti $2\nu = 2(r+1)$ a konfidenční úroveň C.

Hodnota maximální intenzity nebezpečných nediagnostikovaných poruch λ_{DUmax} se určí jako ekvivalent dolní meze intervalu cílové míry poruch PFH pro požadovanou hodnotu SIL, v závislosti na charakteru posuzovaného systému souvisejícího s bezpečností, tedy typu, režimu provozu a uspořádání architektury hardware posuzovaného zařízení.

7.2 Zrychlené zkoušky spolehlivosti bloku logiky

Ukazatel cílové míry poruch je jedním z parametrů hodnocení dosažené úrovně integrity bezpečnosti (SIL) z hlediska náhodných poruch hardware u systémů souvisejících s bezpečností. Hodnota tohoto ukazatele u subsystému bloku logiky modulu UniAVV byla určena na základě informací výrobců o bezporuchovosti jednotlivých tvořících prvků zařízení

(tj. intenzity poruch). Ověření, že tento subsystém skutečně dosahuje požadovaných vlastností funkční bezpečnosti, je vhodné pro uvedený parametr provést realizací zkoušky spolehlivosti.

Cílem uvedené zkoušky spolehlivosti bloku logiky modulu UniAVV je ověřit, zda hlavní faktor ovlivňující parametr cílové míry poruch, tedy hodnota intenzity nebezpečných poruch, která byla zjištěna použitím analytického přístupu na základě informací z průmyslových zdrojů, je ve shodě s reálnou hodnotou tohoto parametru. Z pohledu klasifikace zkoušek spolehlivosti se tedy jedná o zkoušku ověřovací. Vzhledem ke skutečnosti, že na základě výpočtem určené hodnoty bezporuchovosti bloku logiky lze předpokládat doby do poruchy v řádu až desetitisíců hodin, je vhodné za účelem efektivního vyhodnocení skutečné spolehlivosti tohoto subsystému provést tuto zkoušku jako zrychlenou při zvýšené úrovni zatížení.

Vzhledem k charakteru subsystému bloku logiky, který představuje elektronický systém složený z desek s plošnými spoji a procesorovými jednotkami, je vhodné pro zrychlení procesu vzniku poruch provést zkoušku podle Arrheniova modelu, kdy zkouška probíhá při zvýšené teplotě. Model této zkoušky vychází z Arrheniovy rovnice rychlosti reakce a odvozených vztahů pro provádění zrychlených zkoušek u soustav tvořených více prvky, které jsou popsány v kapitole č. 4.2.2.

Tento model představuje nejčastěji používaný přístup při provádění zrychlených zkoušek spolehlivosti elektronických prvků a zařízení. Ve vztahu ke zkoušení subsystému modulu UniAVV lze charakterizovat následující vlastnosti Arrheniova modelu:

- zkouška probíhá při konstantní zvýšené teplotě, další zvýšená zatížení nejsou v modelu obsažena, a tím vede k poměrně jednoduchému a snadno dostupnému zkušebnímu zařízení (tepelná komora),
- charakteristické hodnoty signálů a veličin zkoušeného systému jsou shodné jako při běžných provozních podmínkách, za předpokladu, že zkoušený výrobek je umístěn ve zkušebním stavu simulujícím běžný provoz, vlivy a vazby okolních systémů (např. napájení apod.),
- pro hodnocení provozních podmínek zkoušeného zařízení je dostačující zjistit hodnotu jediného parametru, tj. provozní teplota okolí, při které výrobek plní požadované funkce,
- pro možnost vyhodnocení zkoušky je při běžné realizaci zkoušky nutné určit mechanismus vzniku poruchy a znát hodnotu odpovídající aktivační energie,

- při zkoušce nejsou uvažovány vlivy dalších zatížení, které přispívají k vzniku poruch zařízení (např. vlhkost, vibrace).

Pokud je zrychlená zkouška spolehlivosti s využitím Arrheniova modelu prováděna pouze při jedné úrovni zvýšené teploty, je pro možnost určení faktoru zrychlení zkoušky, který je potřebný pro přepočet parametrů na provozní podmínky, nutné pro každou poruchu zařízení znát hodnotu aktivační energie. Tato hodnota je závislá na typu prvku, u kterého porucha vznikla, a mechanismu vzniku poruchy. Pokud tedy dojde ke vzniku nebezpečné poruchy zkoušeného zařízení (bloku logiky), musí být provedena lokalizace poruchy a následně pro prvek, který poruchu způsobil, také zjištěn typ (způsob) jeho poruchy.

Pokud není možné provádět detailní analýzy způsobů poruch zařízení, nebo pro tvořící prvky nejsou k dispozici příslušné údaje o aktivační energii, je taktéž možné provést zrychlenou zkoušku spolehlivosti využívající Arrheniův model. Avšak za účelem zjištění faktoru zrychlení musí být tato zkouška provedena při dvou různých úrovních zvýšené teploty. Tento přístup s sebou přináší jistý stupeň zjednodušení, kdy jednotlivé reálné prvky zařízení s různými hodnotami aktivačních energií jsou nahrazeny jedním fiktivním blokem charakterizovaným jedinou hodnotou. Další nevýhodu oproti výše uvedenému přístupu představuje zvýšená časová a finanční náročnost provádění zkoušky, kdy zkouška musí být realizována pro dvě skupiny výrobků (postupně nebo současně).

Pro oba výše uvedené přístupy provádění zrychlených zkoušek spolehlivosti byly vypracovány elektronické vyhodnocovací formuláře. Na jejich základě je pro empiricky zjištěné údaje o poruchách získaných ze zkušebního souboru výrobků v průběhu zkoušky proveden intervalový odhad požadovaného parametru bezporuchovosti, tj. intenzity nebezpečných poruch λ_D [h^{-1}]. Formuláře jsou tudíž vhodné pro provedení ověřovací zkoušky spolehlivosti subsystému bloku logiky modulu UniAVV, ale také jakéhokoliv elektronického systému složeného z většího počtu prvků, u nichž se předpokládá exponenciální rozdělení pravděpodobnosti dob do poruchy.

7.2.1 Vyhodnocení zkoušky při znalosti aktivačních energií

Formulář „Arrhenius 1“ (viz příloha č. 5) je určen pro záznam a vyhodnocení zrychlené zkoušky spolehlivosti elektronických systémů, založené na Arrheniově modelu a probíhající při konstantní zvýšené teplotě. Nutnou podmínkou pro jeho použití je znalost všech způsobů poruch, které u jednotlivých tvořících prvků zařízení mohou nastat

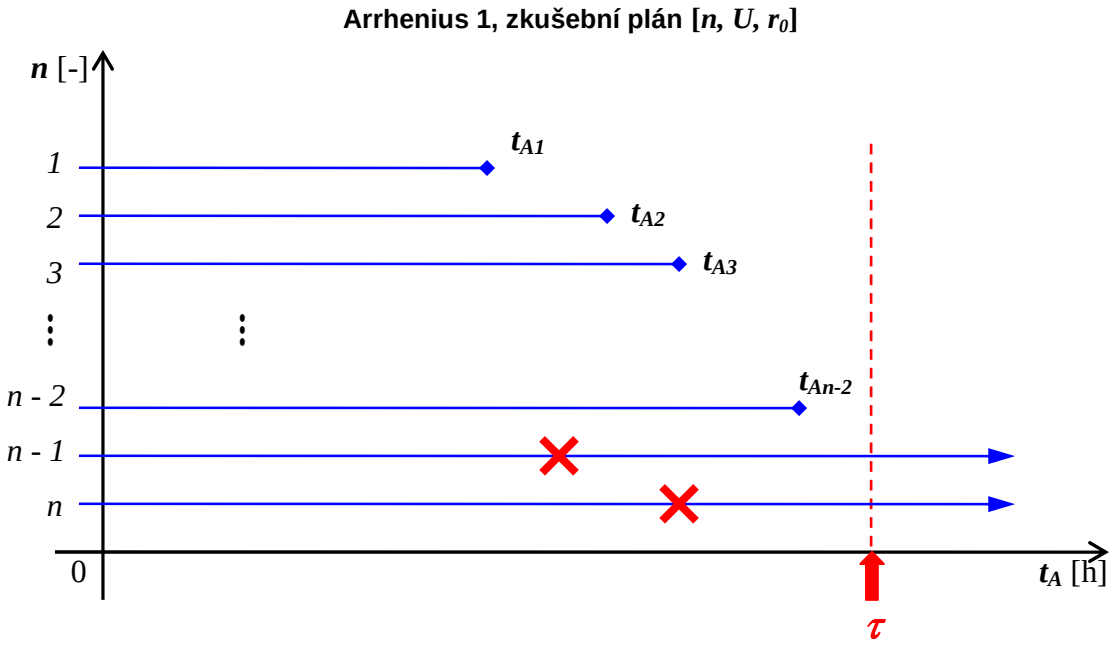
(mechanismy vzniku poruchy), a jim odpovídající hodnoty aktivační energie E_A [eV]. Přehled aktivačních energií běžně používaných elektronických prvků a jejich obvyklých mechanismů poruch je uveden v tabulce č. 7.2 [9].

Tabulka č. 7.2: Aktivační energie mechanismů poruch elektronických prvků

Elektronický prvek **Mechanismus vzniku poruchy**	**Aktivační energie** E_A [eV]
Křemíkové polovodičové prvky	
- akumulace povrchového náboje, bipolární	1,0 ÷ 1,05
- akumulace povrchového náboje, MOS	1,2 ÷ 1,35
- zachycení náboje	1,3 ÷ 1,4
- metalizace	0,5 ÷ 1,2
- elektromigrace	0,5 ÷ 1,2
- koroze (chemická, galvanická, elektrolytická)	0,3 ÷ 0,6
- vazby	1,0 ÷ 1,05
- intermetalický nárůst Al/Au	1,0 ÷ 1,05
Dynamická paměť RAM	
- zachycení náboje	1,0
- kontaminace	1,4
- povrchový náboj	0,5 ÷ 1,0
- elektromigrace	1,0
- defekty oxidů	0,3
Tranzistory FAMOS	
- ztráta náboje	0,8
Integrované obvody MOSFET	
- posun prahového napětí	1,2
Integrované obvody TTL, diody a tranzistory s plochými vývody	0,8 ÷ 2,0
Prvky MOS (včetně PMOS, CMOS)	1,1 ÷ 1,3
GaAs mikrovlnné prvky	
- kontaktní migrace kovů	2,3
Opto-elektronické prvky	
- optocoupler LED	0,4
- optocoupler fototranzistor	1,3
- optocoupler kompozitní	0,6
Diody LED	0,8
Uhlíkové rezistory	0,6
Ohebné plošné spoje	
- ztráta povrchového izolačního odporu (pod 75 ℃)	0,4
- ztráta povrchového izolačního odporu (nad 75 ℃)	1,4
Lineární operační zesilovač	1,6 ÷ 1,8

Zkušební plán zkoušky má označení [n, U, r_0]. Do zkoušky je zařazeno n výrobků, přičemž při vzniku nebezpečné poruchy se nenahrazují. Zkouška probíhá u všech výrobků současně. Konec zkoušky nastává při vzniku poruchy u všech zkoušených výrobků, nebo v případě uplynutí vymezené doby pro provedení zkoušky. V tomto případě, kdy ještě nevznikla porucha u všech zkoušených výrobků, se do výpočtu akumulované pracovní doby zkoušky zahrnují pouze samotné doby do poruchy. Doba činnosti neporušených výrobků do

výpočtu nemůže být zahrnuta z důvodu, že u provozuschopného výrobku není známý mechanismus poruchy a nelze tedy určit faktor zrychlení. Schéma zkušebního plánu je na obr. č. 7.3.

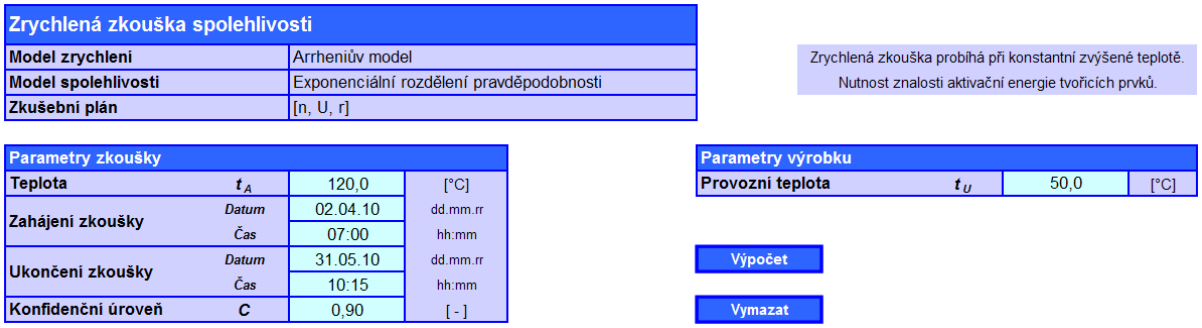


Obr. č. 7.3: Zkušební plán pro zkoušku typu „Arrhenius 1“

Před zahájením zkoušky je nutné zjistit skutečnou provozní teplotu, při které daný systém vykonává požadované funkce. Do formuláře zkoušky se zaznamenává jediný číselný údaj, který představuje typickou hodnotu, případně při intervalovém rozsahu pracovních teplot pak hodnotu průměrnou.

Další vstupní parametr zkoušky představuje zvýšená teplota při zkoušce. Volí se tak, aby byla vyšší než je provozní teplota výrobku a zároveň aby nebyla příliš vysoká, tak aby během zkoušky nevznikaly destrukční poruchy, které se při běžných podmínkách nevyskytují. Podle údajů v dokumentaci o spolehlivosti provádějí výrobci elektronických prvků obvykle zrychlené zkoušky spolehlivosti při teplotě 120 °C. Teplota zkoušky se avšak musí volit s ohledem na informace uvedené v technické dokumentaci tvořících prvků a přizpůsobit se nejméně tepelně odolnému prvku.

Pro účely výpočtu intervalového odhadu je potřeba zadat také hodnotu konfidenční úrovně C z intervalu (0; 1), představující pravděpodobnost, s jakou se kvantitativní parametr bezporuchovosti nachází ve vypočteném intervalu. Výřez formuláře se vstupními údaji pro zkoušku spolehlivosti je zobrazena na obr. č. 7.4.



Zrychlená zkouška spolehlivosti	
Model zrychlení	Arrheniův model
Model spolehlivosti	Exponenciální rozdělení pravděpodobnosti
Zkušební plán	[n, U, r]

Zrychlená zkouška probíhá při konstantní zvýšené teplotě.
Nutnost znalosti aktivační energie tvořicích prvků.

Parametry zkoušky			
Teplota	t_A	120,0	[°C]
Zahájení zkoušky	Datum	02.04.10	dd.mm.rr
	Čas	07:00	hh:mm
Ukončení zkoušky	Datum	31.05.10	dd.mm.rr
	Čas	10:15	hh:mm
Konfidenční úroveň	C	0,90	[-]

Parametry výrobku			
Provozní teplota	t_U	50,0	[°C]

Výpočet

Vymazat

Obr. č. 7.4: Příklad zadávaných údajů pro zrychlenou zkoušku

Zrychlená zkouška spolehlivosti se provádí pro všechny zkoušené výrobky současně. Výrobky jsou připojeny ke zkušebnímu stavu a v okamžiku, kdy teplota v tepelné komoře dosáhne požadované hodnoty, se spustí simulace běžné činnosti zkoušených výrobků. Od tohoto okamžiku, který je zaznamenán do formuláře jako začátek zkoušky, jsou evidovány doby do poruchy výrobků ve zkoušce. Pro jednotlivé výrobky jsou zaznamenány datum a čas vzniku jejich nebezpečné poruchy. Okamžik ukončení zkoušky může být ve formuláři také uveden, má však pouze informativní charakter. Po ukončení zkoušky musí být provedena lokalizace poruchy a analýza typu poruchy. Na jejich základě se pro každou poruchu určí její aktivační energie. Výřez záznamové části formuláře je na obr. č. 7.5.

Průběh zkoušky - záznam poruch				
poř. č.	*Datum*	*Čas*	*Prvek*	*Aktivační energie [eV]*
1	03.04.10	12:30	opto-coupler	0,4
2	04.04.10	03:40	RAM	0,5
3	04.04.10	19:00	tranzistor	1,0
4	05.04.10	12:15	MOS	1,1
5	07.04.10	03:35	dioda	0,8
6	08.04.10	14:05	rezistor	0,6
7	28.04.10	07:30	tranzistor	1,0
8	16.05.10	16:25	opto-coupler	0,6
9	28.05.10	23:40	dioda	0,8
10	31.05.10	10:15	tranzistor	1,0
11				
12				

Obr. č. 7.5: Příklad zadávání údajů o poruchách výrobků

Po skončení zkoušky a vyplnění všech požadovaných údajů je možné tlačítkem „Výpočet“ spustit algoritmus výpočtu. Výstupem je intervalový odhad intenzity

nebezpečných poruch určený pro zkušební podmínky, který je s využitím Arrheniova převodního vztahu přepočten na požadovaný jednostranný odhad intenzity nebezpečných poruch zařízení pro uvedenou provozní teplotu a požadovanou konfidenční úroveň. S využitím převodního vztahu pro exponenciálního rozdělení je určena také dolní mez intervalového odhadu střední doby do poruchy. Jako informativní údaj je vypočtena hodnota středního faktoru zrychlení realizované zkoušky. Tento údaj nezohledňuje rozdílné hodnoty aktivačních energií jednotlivých poruch, charakterizuje systém, pokud by byl tvořen jediným prvkem. Výřez výsledkové části formuláře je na obr. č. 7.6.

Vyhodnocení zkoušky				
Zkušební podmínky				
Intenzita poruch	λ_A	≤	3,113E-03	[h^{-1}]
Provozní podmínky				
Intenzita poruch	λ_U	≤	**9,339E-06**	[h^{-1}]
Střední doba do poruchy	T_S	≥	**107079,6**	[h]
Střední faktor zrychlení	A_F		333,35	[-]

Obr. č. 7.6: Příklad vyhodnocení zrychlené zkoušky

7.2.2 Vyhodnocení zkoušky bez znalosti aktivačních energií

V případech, kdy u zkoušených výrobků není možné zcela identifikovat možné způsoby poruch jejich tvořících prvků, nebo pro určitý mechanismus poruchy není známá odpovídající hodnota aktivační energie, je přesto možné použít zrychlenou zkoušku spolehlivosti využívající Arrheniův model pro ověření požadovaného parametru bezporuchovosti. Tento přístup je však spojen s některými omezeními, nižší přesností a vyšší časovou nebo finanční zátěží než při provádění zrychlené zkoušky popsané výše.

Pokud není možné pro určitý způsob poruchy tvořícího prvku elektronického systému určit hodnotu aktivační energie, není možné aplikovat Arrheniův převodní vztah za účelem výpočtu faktoru zrychlení. Aby bylo možné určit faktor zrychlení zkoušky, s jehož využitím se provádí převod výsledků získaných při zvýšeném zatížení na hodnoty pro běžné provozní zatížení, je nutné provádět zkoušku spolehlivosti při dvou rozdílných teplotách. Tímto postupem se stanoví odhad aktivační energie zkoušeného zařízení.

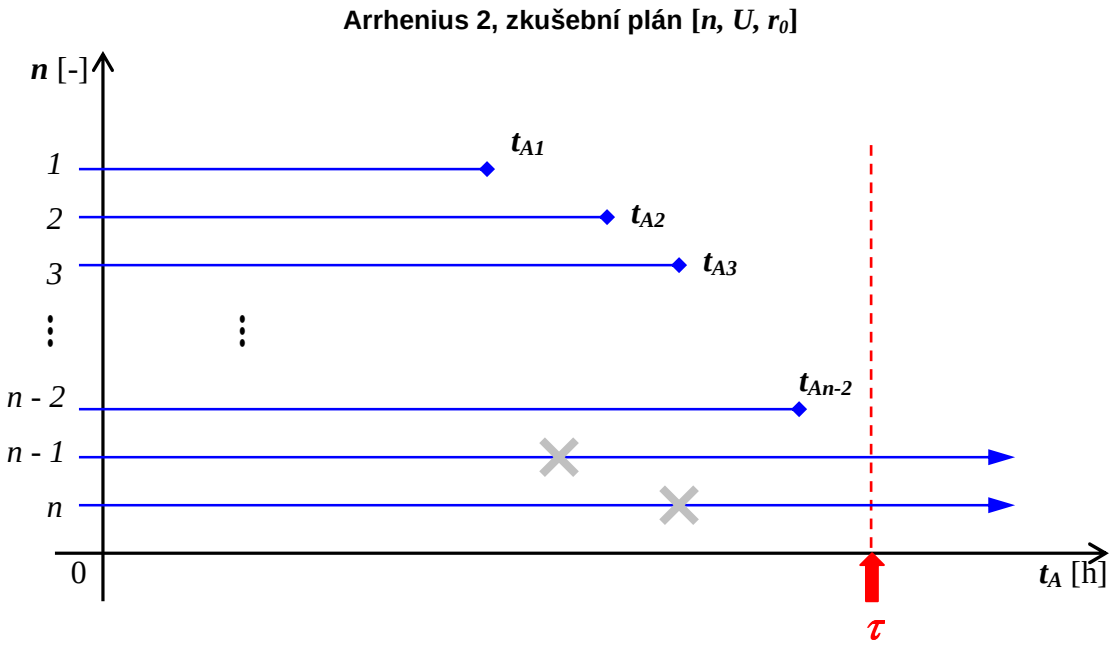
Vzhledem ke skutečnosti, že elektronická zařízení (včetně subsystému bloku logiky modulu UniAVV) jsou tvořena velkým počtem různorodých prvků, přičemž aktivační energie jejich poruch není konstantní, je zřejmé, že použitím tohoto postupu dochází k jisté míře zjednodušení a nižší přesnosti dosaženého výsledku. Při aplikaci tohoto přístupu je vícečlenný systém nahrazen jediným „fiktivním“ blokem, který je charakterizován jednou hodnotou aktivační energie. Proto je vhodné tuto metodu využít v případech, kdy systém je z velké části tvořen elektronickými prvky stejného typu, nebo kdy se předpokládá rozložení hodnot příslušných aktivačních energií v úzkém intervalu.

Dalším omezením provedení zrychlené zkoušky spolehlivosti uvedeným postupem je nutnost její realizace při dvou rozdílných úrovních zvýšené teploty. Je-li k dispozici pouze jedno zkušební zařízení (tepelná komora), je realizace zkoušky spojena se značným zvětšením jejího časového rozsahu. Zkouška musí proběhnout postupně pro dvě rozdílné teploty, přičemž při nižší zkušební teplotě dochází k úměrnému prodloužení dob do poruchy zkoušených výrobků. Nižší časovou náročnost představuje provedení zkoušky ve dvou zkušebních zařízeních, kdy zkouška může probíhat pro oba zkušební soubory současně. To s sebou přináší vyšší náklady na pořízení (nebo pronájem) dvou tepelných komor, přičemž doba zkoušky je delší oproti provádění zkoušky při znalosti příslušných aktivačních energií.

I přes výše uvedená omezení je uvedená metoda provádění zrychlených zkoušek vhodná pro snadné ověření parametrů bezporuchovosti zkoušených výrobků, zejména v případech, kdy z různých důvodů není k dispozici dostatečné množství informací o mechanismu vzniku poruch tvořících prvků, nebo nejsou dostatečné kapacity pro možnost následné lokalizace a analýzy poruch u zkoušených výrobků. Pro záznam a vyhodnocení zrychlené zkoušky spolehlivosti je použit elektronický formulář „Arrhenius 2“ (uvedený jako příloha č. 6).

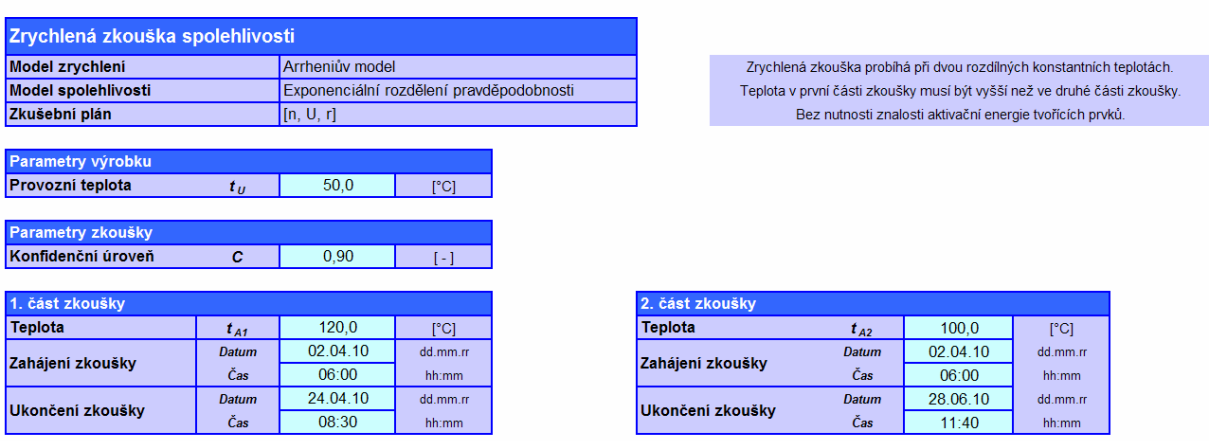
Zrychlená zkouška probíhá nezávisle pro dva zkušební soubory podle zkušebního plánu s označením [n, U, r]. V průběhu zkoušky se výrobky, u kterých vznikne porucha, nenahrazují a zkouška končí při poruše všech zkoušených výrobků. V případě, že je doba zkoušky omezena maximální dobou trvání, je možné transformovat zkušební plán na typ [n, U, τ]. V tomto případě je do akumulované pracovní doby zkoušky možné započítat také doby provozu výrobků, u kterých během zkoušky nevznikla porucha. To je možné na základě předpokladu, že všechny poruchy prvků jsou reprezentovány jednou „střední“ hodnotou aktivační energie, proto se u všech dob do poruchy předpokládá shodný faktor zrychlení. Soubor zjištěných hodnot by tak představoval cenzurovaný soubor dat omezený dobou trvání

zkoušky. Avšak pro zachování shodné metodiky vyhodnocování zkoušky jako u výše uvedeného modelu „Arrhenius 1“ jsou do akumulované doby zkoušky zahrnuty pouze doby provozu těch výrobků, u kterých vznikla porucha. Schéma zkušebního plánu pro dílčí zkoušku (jednu úroveň zvýšené teploty) je uveden na obr. č. 7.7.



Obr. č. 7.7: Zkušební plán pro dílčí zkoušku typu „Arrhenius 2“

Zadávání parametrů zrychlené zkoušky (konfidenční úroveň) a provozních parametrů zkoušeného výrobku (provozní teplota) je shodné jako u předešlého formuláře „Arrhenius 1“. Dalšími vstupními parametry zadávanými před realizací zkoušky jsou dvě rozdílné úrovně zvýšené teploty. Algoritmus výpočtu hledaných parametrů bezporuchovosti je založen na požadavku, aby teplota v první části zkoušky byla vyšší než v části druhé. V první části zkoušky je tedy teplota volena nejvyšší možná v závislosti na tepelné odolnosti tvořících prvků (podle technické dokumentace výrobků). V druhé části zkoušky musí být nižší teplota volena s ohledem na dostatečnou diferenciaci od hodnoty vyšší pro věrohodný odhad střední aktivační energie, ale ne příliš nízká, což snižuje zrychlující účinek zkoušky a prodlužuje dobu jejího trvání. Výřez formuláře pro zadávání vstupních hodnot zkoušky je uveden na obr. č. 7.8.



Zrychlená zkouška spolehlivosti	
Model zrychlení	Arrheniův model
Model spolehlivosti	Exponenciální rozdělení pravděpodobnosti
Zkušební plán	[n, U, r]

Zrychlená zkouška probíhá při dvou rozdílných konstantních teplotách.
Teplota v první části zkoušky musí být vyšší než ve druhé části zkoušky.
Bez nutnosti znalosti aktivační energie tvořících prvků.

Parametry výrobku			
Provozní teplota	t_U	50,0	[°C]

Parametry zkoušky			
Konfidenční úroveň	C	0,90	[-]

1. část zkoušky			
Teplota	t_{A1}	120,0	[°C]
Zahájení zkoušky	Datum	02.04.10	dd.mm.rr
	Čas	06:00	hh:mm
Ukončení zkoušky	Datum	24.04.10	dd.mm.rr
	Čas	08:30	hh:mm

2. část zkoušky			
Teplota	t_{A2}	100,0	[°C]
Zahájení zkoušky	Datum	02.04.10	dd.mm.rr
	Čas	06:00	hh:mm
Ukončení zkoušky	Datum	28.06.10	dd.mm.rr
	Čas	11:40	hh:mm

Obr. č. 7.8: Příklad zadávaných údajů pro zrychlenou zkoušku

Při provádění zkoušky je zaznamenán čas začátku zkoušky pro obě skupiny zkoušených výrobků, kdy teplota v komoře dosáhne požadované hodnoty. V tomto okamžiku je spuštěna simulace činnosti výrobků ve zkušebních stavech a je zaznamenáváno datum a čas vzniku jednotlivých nebezpečných poruch zkoušených výrobků. Toto jsou dostačující informace pro provedení výpočtu hledaných ukazatelů bezporuchovosti. Okamžik ukončení zkoušky má pouze informativní charakter. Tento parametr by měl význam v případě transformace zkušebního plánu na typ *t*-plánu (viz výše). Výřez z formuláře pro evidenci průběhu zkoušky je na obr. č. 7.9.

1. část zkoušky		
Průběh zkoušky - záznam poruch		
poř. č.	Datum	Čas
1	03.04.10	14:50
2	04.04.10	23:10
3	06.04.10	18:25
4	07.04.10	01:00
5	07.04.10	22:05
6	10.04.10	16:20
7	16.04.10	06:10
8	24.04.10	08:30
9		
10		
11		

2. část zkoušky		
Průběh zkoušky - záznam poruch		
poř. č.	Datum	Čas
1	09.04.10	18:25
2	10.04.10	01:30
3	12.04.10	23:05
4	18.04.10	15:45
5	26.04.10	06:25
6	18.05.10	19:25
7	26.05.10	02:15
8	28.06.10	11:40
9		
10		
11		

Obr. č. 7.9: Příklad zadávání údajů o poruchách výrobků

Po ukončení obou částí zkoušky je tlačítkem „Výpočet“ spuštěn algoritmus pro získání jejich výsledků. S využitím Arrheniova převodního vztahu je ze dvou souborů experimentálně zjištěných dat určena hodnota ekvivalentu aktivační energie, na jejímž základě je vypočten

faktor zrychlení pro jednotlivé části zkoušky. Pokud by zkoušený výrobek představoval jednoprvkový systém s jedním dominantním způsobem poruchy, pak zkoušením těchto výrobků ve dvou zkušebních souborech při dvou různých zvýšených teplotách lze model „Arrhenius 2“ využít také pro kvalifikovaný odhad aktivační energie daného mechanismu poruchy.

Na základě znalosti faktoru zrychlení pro obě části zkoušky jsou přepočteny získané hodnoty dob do poruchy pro provozní teplotu výrobku a s využitím chí-kvadrát statistiky vypočteny parametry jeho bezporuchovosti. Ty představují jednostranný intervalový odhad střední doby do nebezpečné poruchy, resp. intenzity nebezpečných poruch na stanovené konfidenční úrovni. Výsledek představuje interval, v němž se hledaný parametr bezporuchovosti celé populace výrobků nachází s danou, předem stanovenou pravděpodobností. Výřez formuláře s výsledky zkoušky je na obr. č. 7.10.

Vyhodnocení zkoušky			
Zkušební podmínky - 1. část			
Intenzita poruch	λ_{A1}	5,241E-03	[h^{-1}]
Zkušební podmínky - 2. část			
Intenzita poruch	λ_{A2}	1,312E-03	[h^{-1}]
Provozní podmínky			
Intenzita poruch	λ_U	≤ 2,725E-05	[h^{-1}]
Stř. doba do poruchy	T_S	≥ 36692,3	[h]
Ekv. aktivační energie	E_A	0,876	[eV]

Obr. č. 7.10: Příklad vyhodnocení zrychlené zkoušky

Poznámka: Data zaznamenaná ve formuláři „Arrhenius 2“, která jsou zobrazena ve výše uvedených příkladech, nejsou zjištěna realizací zkoušky spolehlivosti, ale jsou získána na základě numerické simulace dob do poruchy víceprvkového systému, s cílem demonstrace funkčnosti uvedeného modelu (shodně také pro formulář „Arrhenius 1“).

7.2.3 Řešení software vyhodnocovacích formulářů

Elektronické formuláře „Arrhenius 1“ a „Arrhenius 2“, určené pro vyhodnocování zrychlených zkoušek spolehlivosti elektronických systémů, jsou vytvořeny v programu Microsoft Excel s využitím maker v programovacím jazyku Visual Basic.

Posloupnost realizace programu lze u obou formulářů rozdělit na vstupní část kontroly zadaných parametrů a načtení vložených dat o průběhu zkoušky, procesní část provádění pomocných výpočtů a závěrečnou část výpočtu požadovaných parametrů bezporuchovosti a grafického zobrazení tohoto výsledku. Vývojové diagramy řešení software jednotlivých elektronických formulářů jsou uvedeny na obr. č. 7.11, resp. obr. č. 7.12.

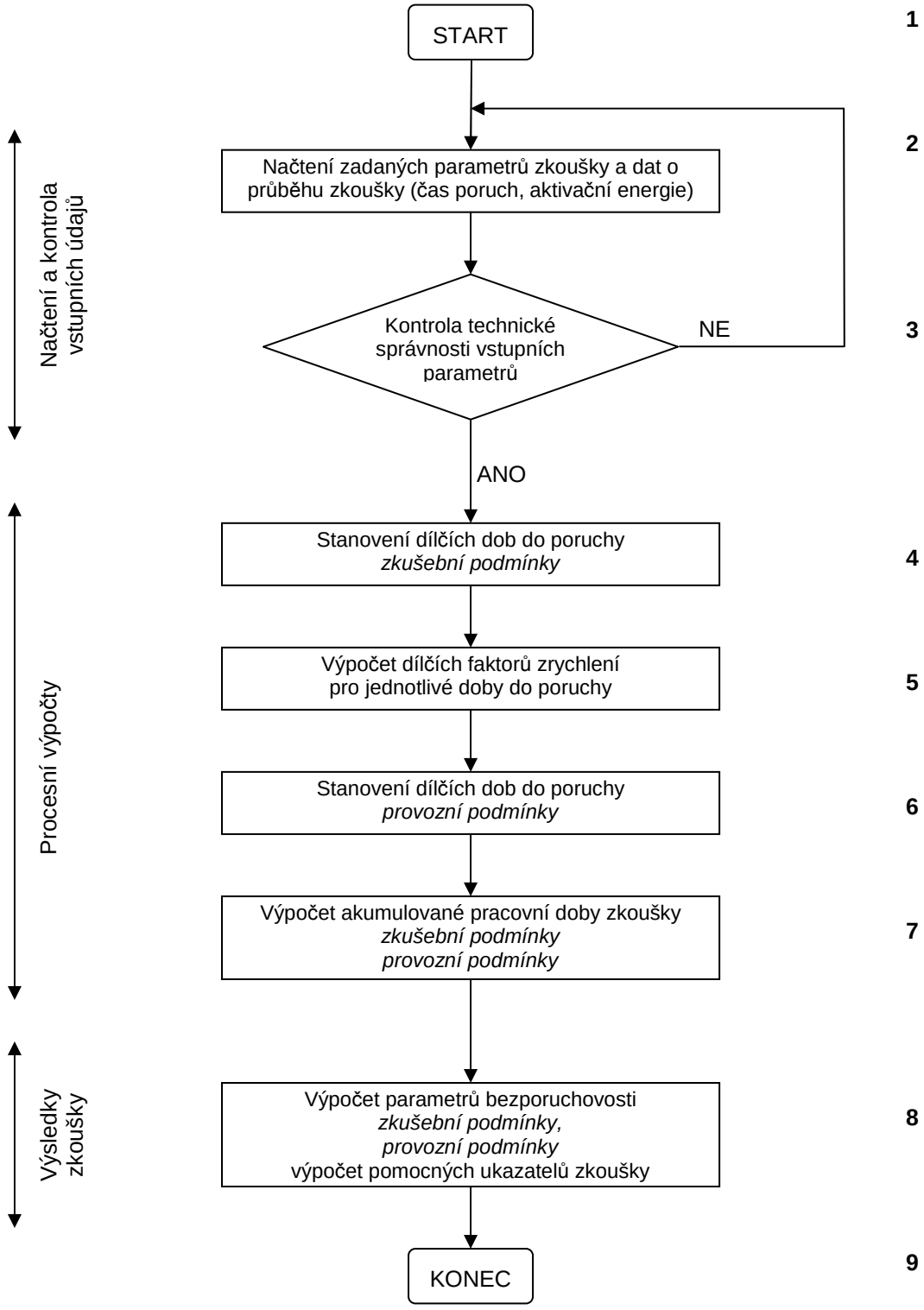
Po zadání vstupních parametrů zkoušky a zaznamenání jejího průběhu je možné spustit algoritmus výpočtu parametrů bezporuchovosti. V úvodní části je provedena technická kontrola správnosti zadaných hodnot, tedy zda se uvedené parametry nalézají ve vymezených intervalech apod. Například konfidenční úroveň C představující pravděpodobnost může nabývat hodnot z intervalu $(0; 1)$. V případě nedodržení tohoto požadavku je uživatel formuláře upozorněn na nutnost provedení opravy. V případě splnění požadavků vstupní kontroly jsou načteny hodnoty průběhu zrychlené zkoušky zadané uživatelem, tj. datum a čas vzniku jednotlivých poruch objektů, případně aktivační energie jejich porušených tvořících prvků.

Ve výpočtové části algoritmu jsou určeny doby do poruchy jednotlivých objektů testovaných ve zrychlené zkoušce spolehlivosti (při zvýšené teplotě) a následně jsou vypočteny hodnoty parametrů (faktor zrychlení), s jejichž využitím jsou uvedené hodnoty dob do poruchy přepočteny na běžné provozní podmínky. Jednotlivé doby do poruchy jsou vypočteny jako rozdíl okamžiku vzniku dané poruchy a okamžiku začátku zrychlené zkoušky. Teoretický model použitý pro elektronický formulář „Arrhenius 1“ umožňuje do výpočtu zařadit pouze necenzurovaný soubor dat, tj. pouze doby do poruchy. Naproti tomu teoretický model formuláře „Arrhenius 2“ dovoluje pro výpočet využít také dobou zkoušky cenzurovaná data, tedy také doby provozu objektů po dobu trvání zkoušky (bez vzniku poruchy). Je-li zvolen pro vyhodnocení zkoušky spolehlivosti uvedený přístup, je nutné zadat mimo okamžiku začátku zkoušky také čas ukončení zkoušky, který je v ostatních případech pouze informativní.

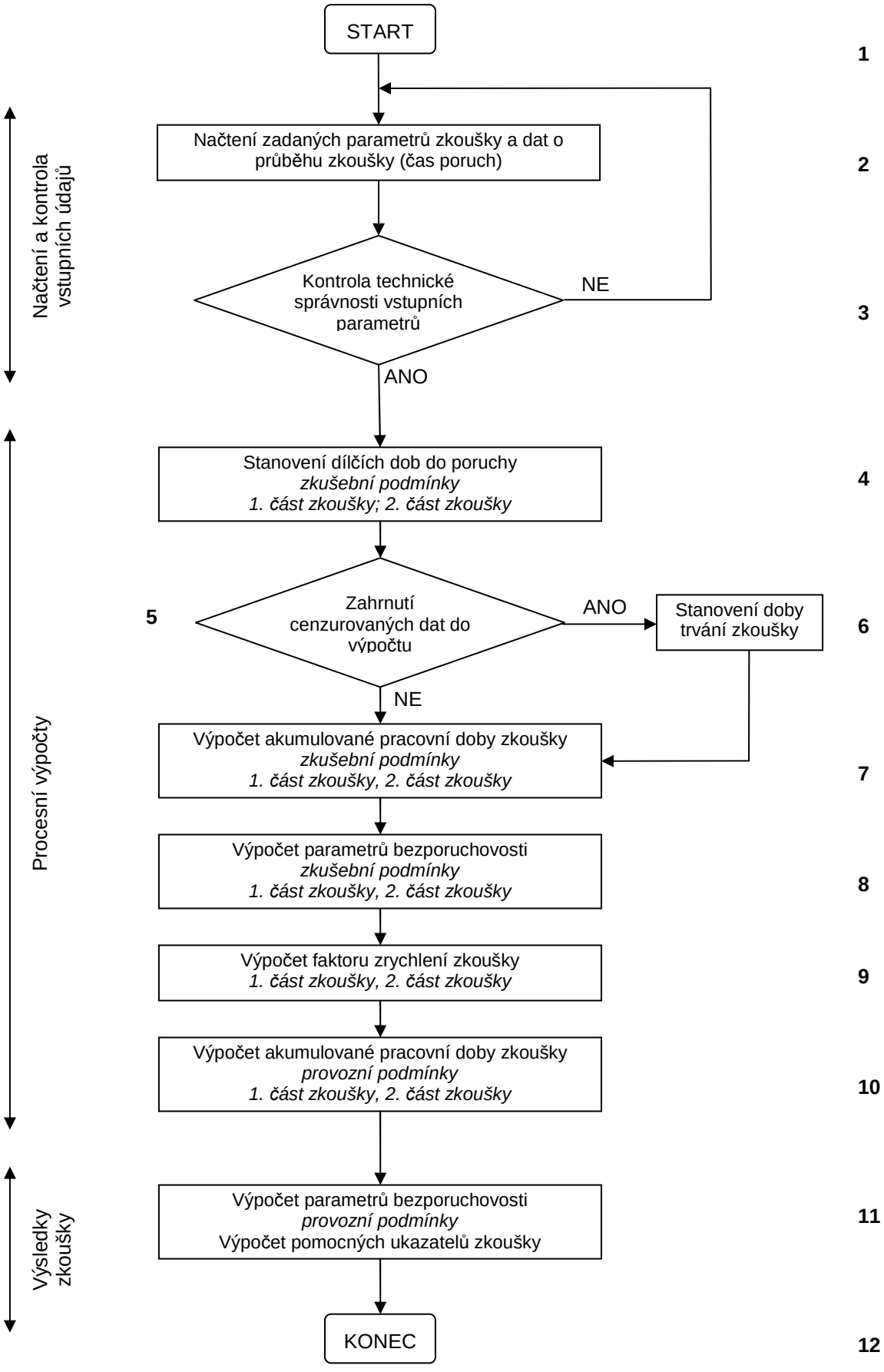
Výše uvedené vypočtené pomocné hodnoty představují vstupní hodnoty pro stanovení intervalových odhadů parametrů bezporuchovosti, jež jsou výsledkem zrychlené zkoušky spolehlivosti. Vypočtené výsledky jsou zobrazeny ve formě tabulky, včetně doplňkových parametrů zkoušky (střední faktor zrychlení, resp. ekvivalentní aktivační energie).

Pozn.: Technická funkčnost elektronických vyhodnocovacích formulářů „Arrhenius 1“ a „Arrhenius 2“ byla ověřena s využitím simulovaných souborů dat. Verifikace faktické

správnosti dosažených výsledků byla provedena realizací analytických výpočtů pro shodné soubory dat.



Obr. č. 7.11: Vývojový diagram formuláře „Arrhenius 1“



Obr. č. 7.12: Vývojový diagram formuláře „Arrhenius 2“

7.2.4 Vyhodnocení ověřovací zkoušky

Cílem ověřovacích zkoušek spolehlivosti, které jsou realizovány jako zrychlené s využitím výše uvedených modelů, je se stanovenou pravděpodobností potvrdit nebo zamítnout hypotézu, že elektronický systém (v tomto případě subsystém bloku logiky modulu UniAVV) dosahuje předpokládané úrovně bezporuchovosti, charakterizované hodnotou intenzity nebezpečných poruch. Provedením zkoušky spolehlivosti pro zkušební soubor několika náhodně vybraných výrobků lze na dané konfidenční úrovni přijmout rozhodnutí ve vztahu ke všem vyrobeným výrobkům, tedy celé populaci.

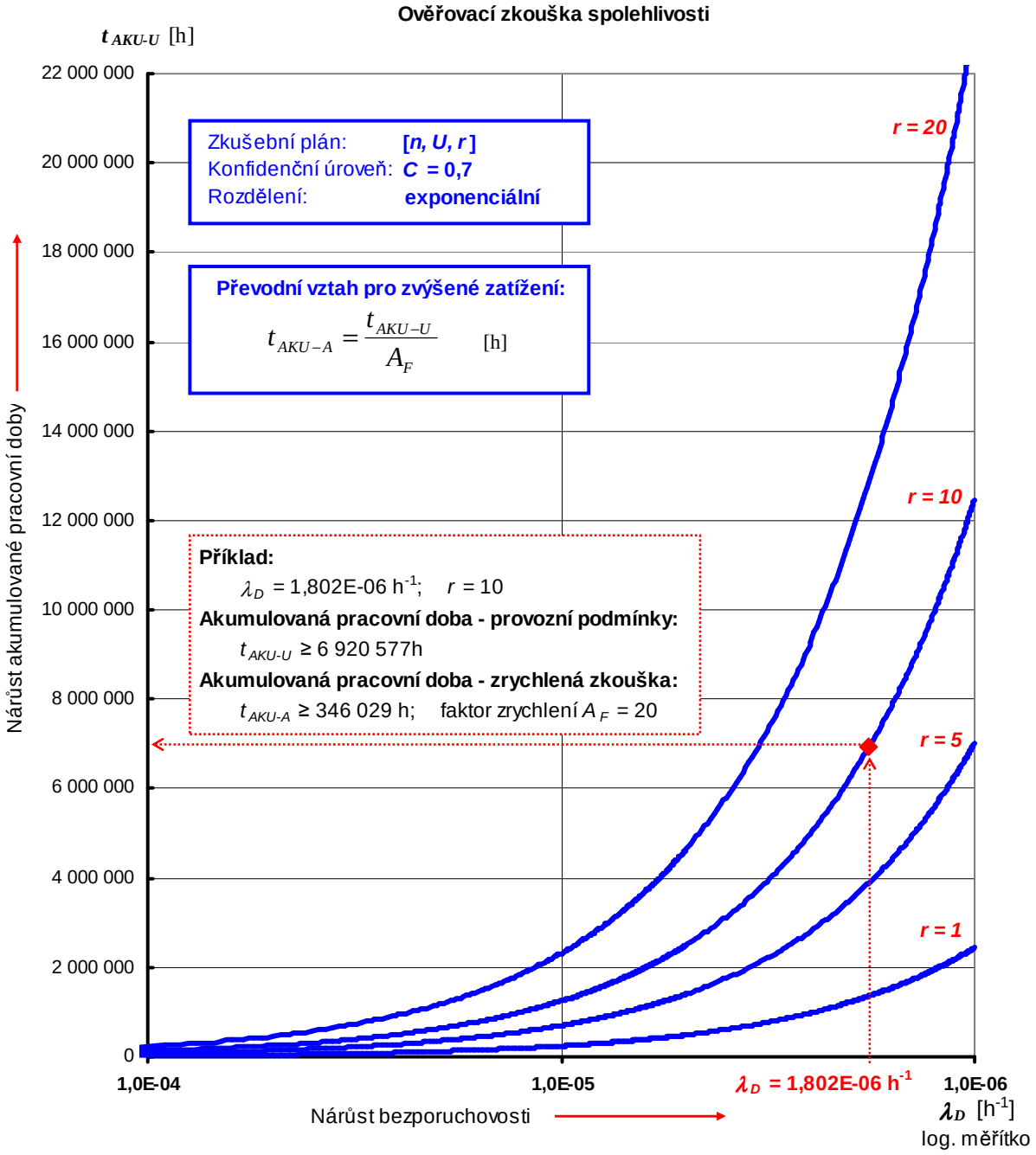
Vzhledem ke skutečnosti, že u systémů tvořených elektronickými prvky lze předpokládat exponenciální rozdělení pravděpodobnosti dob do poruchy a tedy parametr intenzity poruch je konstantní, je vyhodnocení provedených ověřovacích zkoušek spolehlivosti jednoznačné a snadné. Pokud je hodnota intenzity nebezpečných poruch výrobku λ_D [h^{-1}] zjištěná experimentálně provedením zkoušky spolehlivosti nižší nebo rovna hodnotě tohoto parametru vypočtené analytickou metodou s využitím informací z průmyslových zdrojů, lze s pravděpodobností odpovídající stanovené konfidenční úrovni C potvrdit, že populace daného výrobku dosahuje předpokládané úrovně bezporuchovosti, neboli:

$$\lambda_{D-Test} \leq \lambda_{D-Model} \qquad [\mathrm{h}^{-1}] \tag{7.13}$$

Pokud z určitých důvodů nelze pro provedení ověřovací zkoušky spolehlivosti využít výše uvedených modelů „Arrhenius 1“ nebo „Arrhenius 2“, např. z důvodu odlišného zkušebního plánu (výrobky jsou zkoušeny individuálně s různými počátky zkoušek), nebo z důvodu použití jiného než Arrheniova převodního vztahu zrychlení zkoušky, je výhodné pro její vyhodnocení zvolit univerzální přístup založený na posouzení akumulované pracovní doby zkoušky t_{AKU} [h].

Tento přístup v sobě slučuje použití libovolného zkušebního plánu (t-plán, r-plán) a některého z modelů zrychlení zkoušky, charakterizovaného faktorem zrychlení A_F. Použitím tohoto přístupu lze na dané konfidenční úrovni stanovit minimální požadovanou akumulovanou pracovní dobu výrobků zařazených do zkoušky t_{AKU} [h], aby se stanovenou pravděpodobností mohla být prokázána požadovaná hodnota intenzity nebezpečných poruch λ_D [h^{-1}]. Před aplikací tohoto postupu musí být avšak stanoveny podmínky, za kterých zkouška probíhá.

Před provedením zkoušky musí být definovány parametry zkušebního plánu (počet výrobků ve zkoušce, režim nahrazování výrobků, podmínky ukončení zkoušky apod.), stanovena hodnota konfidenční úrovně C a musí být známa hodnota faktoru zrychlení zkoušky A_F. Pak lze vyjádřit parametr akumulované pracovní doby jako funkci intenzity nebezpečných poruch, pro praktické účely vhodně ve formě tabulky nebo grafického vyjádření (viz obr. č. 7.13).



Obr. č. 7.13: Závislost akumulované pracovní doby na intenzitě poruch

V uvedeném grafu je zaznamenán průběh závislosti akumulované pracovní doby na intenzitě nebezpečných poruch pro zkušební plán [*n*, *U*, *r*]. Zkouška v tomto případě končí při poruše všech výrobků do ní zařazených.

Zobrazená akumulovaná pracovní doba $t_{AKU\text{-}U}$ [h] představuje součet dob do poruchy zkoušených výrobků, pokud je zkouška prováděná při běžných provozních podmínkách. Převod tohoto parametru do podmínek zrychlené zkoušky se provádí s využitím faktoru zrychlení zkoušky A_F. Akumulovaná pracovní doba zrychlené zkoušky $t_{AKU\text{-}A}$ [h] je tedy násobně nižší, nepřímo úměrně A_F, a je dána vztahem:

$$t_{AKU-A} = \frac{1}{A_F} \cdot t_{AKU-U} \quad [\text{h}] \qquad (7.14)$$

Například pro prokázání předpokládané analyticky zjištěné intenzity nebezpečných poruch o hodnotě $\lambda_D = 1{,}802.10^{-6}$ [h^{-1}] na konfidenční úrovni $C = 0{,}7$ by akumulovaná pracovní doba zkoušky, ve které by bylo zařazeno 10 výrobků, musela dosáhnout minimálně 6 920 577 hodin při provozních podmínkách, resp. 346 029 hodin při zvýšeném zatížení a známém faktoru zrychlení $A_F = 20$.

Obecně lze výše uvedenou závislost vyjádřit pomocí vztahu (7.15), ve kterém v souvislosti s intervalovým odhadem intenzity nebezpečných poruch vystupuje statistika chí-kvadrát. Její hodnota je závislá na počtu poruch *r*, které u zkušebního souboru výrobků vzniknou v průběhu zkoušky, a na stanovené konfidenční úrovni *C*. Je s výhodou použitelná jak pro necenzurované, tak i cenzurované soubory dat.

$$t_{AKU-A} = \frac{1}{\lambda_D} \cdot \frac{\chi^2_{2(r+1);\,C}}{2} \cdot \frac{1}{A_F} \quad [\text{h}] \qquad (7.15)$$

kde: $t_{AKU\text{-}A}$ – akumulovaná pracovní doba výrobků ve zkoušce při zvýšeném zatížení [h],
λ_D – intenzita nebezpečných poruch zjištěná analytickou metodou [h^{-1}],
A_F – faktor zrychlení zkoušky [-],
χ^2 – hodnota chí-kvadrát statistiky pro počet stupňů volnosti *2(r + 1)* a konfidenční úroveň *C*.

Výše uvedený přístup hodnocení zkoušek spolehlivosti elektronických systémů představuje poměrně jednoduchý přístup pro případy, kdy nelze použít dříve popsané modely. Z důvodu možnosti zpracování v tabulkové nebo grafické formě představuje vhodný nástroj pro ověření dosažené úrovně bezporuchovosti, aniž by bylo nutné aplikovat složitý matematický aparát a je tudíž vhodný pro praktické využití v průmyslovém prostředí.

8 ZÁVĚR

Náplní této disertační práce bylo provedení kvalitativní a kvantitativní analýzy spolehlivosti modulu UniAVV, jež je centrální řídící a diagnostickou jednotkou systému automatického vedení vlaku. Pro ověření skutečné úrovně vybraných parametrů spolehlivosti tohoto zařízení byl navržen program zkoušek spolehlivosti a vytvořen software pro jejich vyhodnocování. Pro hodnocení spohlivosti modulu UniAVV byly zvoleny postupy a nástroje, jež vycházejí z principů funkční bezpečnosti elektrických/elektronických systémů souvisejících s bezpečností, popsaných v normě ČSN EN 61508.

Při kvalitativním hodnocení spolehlivosti modulu UniAVV byly s využitím analýzy způsobů a důsledků poruch (FMEA) identifikovány jednotlivé funkce modulu a způsoby jejich selhání. U funkcí, jejichž selhání může způsobit ohrožení bezpečnosti železniční dopravy, bylo provedeno kvalitativní hodnocení rizika metodou diagramu rizika. Výstupem této analýzy byly požadavky na opatření vedoucí ke snížení rizika na společensky přijatelnou úroveň, které jsou definovány s využitím ukazatele úrovně integrity bezpečnosti (SIL). Z výsledků analýzy subsystémů modulu UniAVV vyplynulo, že pro účinnou eliminaci rizika vyplývající ze selhání jejich funkcí musí být dosažena úroveň SIL2. Pro variantní uspořádání architektury hardware subsystémů modulu UniAVV byly specifikovány požadavky na kvalitu a účinnost diagnostického systému a definovány krajní meze kvantitativních ukazatelů bezporuchovosti podle principů funkční bezpečnosti.

Cílem kvantitativní analýzy spolehlivosti modulu UniAVV bylo vytvoření teoretického modelu bezporuchovosti pro náhodné poruchy hardware, na jehož základě byly výpočtem určeny konkrétní číselné hodnoty ukazatelů funkční bezpečnosti. Na základě vypočteného diagnostického pokrytí modulu UniAVV, charakterizujícího kvalitu diagnostického systému, a informací z průmyslových zdrojů o intenzitách poruch tvořících prvků hardware byla určena číselná hodnota ukazatele cílové míry poruch. S ohledem na konkrétní technické provedení modulu UniAVV bylo zjištěno, že hodnoty diagnostického pokrytí a cílové míry poruch vyhovují požadavku úrovně integrity bezpečnosti SIL2.

Pro možnost ověření skutečně dosažené úrovně spolehlivosti modulu UniAVV byly navrženy programy zkoušek spolehlivosti. Ty umožňují vyhodnocení dat získaných jak během provozu modulu UniAVV, tak také dat získaných v laboratorních podmínkách ze zkoušek prováděných při nadměrném zatížení. Pro snadné určení výsledků realizovaných

zkoušek spolehlivosti byl vytvořen softwarový nástroj ve formě elektronických formulářů, umožňující vyhodnocení zkoušek prováděných v různých režimech zatížení.

Prokázáním a ověřením dosažené úrovně integrity bezpečnosti SIL2 u modulu UniAVV lze deklarovat konkrétní číselné hodnoty ukazatelů spolehlivosti, které tento systém dosahuje. Pravděpodobnost nebezpečné nediagnostikované poruchy dosahuje u modulu UniAVV hodnoty nejméně desetinásobně nižší než by byla u systému s prokázanou úrovní integrity bezpečnosti SIL1 a hodnoty minimálně stonásobně nižší než u systému, který hodnoty SIL1 nedosahuje. Uvedená pravděpodobnost je úměrná pravděpodobnosti vzniku nebezpečné události, kterou může nebezpečná nediagnostikovaná porucha modulu UniAVV vyvolat. Ta může v krajním případě vést k ohrožení bezpečnosti železniční dopravy, a tedy k újmám na lidských životech a zdraví a značným hmotným škodám. U modulu UniAVV s prokázanou úrovní integrity bezpečnosti SIL2 je tedy pravděpodobnost vzniku nákladů spojených s uvedenými důsledky ohrožení bezpečnosti mnohonásobně nižší než u systému, který požadované úrovně funkční bezpečnosti nedosahuje.

8.1 Přínosy práce pro vědu a praxi

Hodnocení spolehlivosti a bezpečnosti modulu UniAVV bylo v této disertační práci provedeno v souladu s mezinárodní normou ČSN EN 61508 Funkční bezpečnost elektrických /elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Výstupy této práce tak mohou být využity jako součást dokumentace potřebné pro prokázání dosažené úrovně integrity bezpečnosti (SIL) tohoto modulu, zejména část věnující se kvalitativnímu hodnocení rizika a stanovení požadavků bezpečnosti a část popisující určení číselných hodnot ukazatelů funkční bezpečnosti pro náhodnou poruchu hardware. Tato dokumentace je nezbytná pro proces certifikace výrobku, potvrzující jeho vlastnosti z hlediska požadavků funkční bezpečnosti.

Na základě této dokumentace může výrobce modulu UniAVV, společnost MSV elektronika s.r.o., zažádat o certifikaci tohoto produktu z hlediska norem funkční bezpečnosti pro dosaženou úroveň integrity bezpečnosti SIL2. Této hodnotě SIL vyhovuje modul UniAVV jak z hlediska účinnosti svého diagnostického systému (popsaného ukazatelem diagnostického pokrytí), tak i z hlediska požadované bezporuchovosti (dané ukazatelem cílové míry náhodných poruch hardware). Toto hodnocení funkční bezpečnosti modulu UniAVV je založeno na provedené analýze způsobů a důsledků poruch (FMEA) jeho funkcí,

kvalitativním hodnocení rizika ve spojitosti s bezpečností železničního provozu a na vytvořeném teoretickém modelu bezporuchovosti, které jsou obsaženy v této práci.

Vzhledem k použitému technickému řešení modulu UniAVV muselo být toto zařízení jako celek pojato jako systém související s bezpečností, a proto všechny jeho subsystémy a součásti musely vyhovět náročným požadavkům funkční bezpečnosti. Uvedené výsledky analýz spolehlivosti modulu UniAVV tak mohou jeho výrobci sloužit jako podklad pro případné konstrukční změny systému, které by umožnily realizovat systém související s bezpečností jako nezávislý na modulu UniAVV. Tímto přístupem by se při zachování stávající úrovně integrity bezpečnosti značně zmírnily požadavky na parametry spolehlivosti tvořících prvků modulu UniAVV.

Pro možnost ověření skutečné úrovně spolehlivosti, zejména parametrů bezporuchovosti modulu UniAVV byl v této práci navržen program provádění zkoušek spolehlivosti. Postup a podmínky provádění byl stanoven jak pro zkoušky prováděné v běžných provozních podmínkách, tak také pro zkoušky zrychlené, prováděné při nadměrném zatížení, konkrétně zvýšené teplotě. Výstupem zkoušek realizovaných podle vytvořených programů je intervalový odhad parametrů bezporuchovosti na zvolené konfidenční úrovni.

Pro určení, resp. ověření úrovně spolehlivosti vycházející z provozních informací subsystémů modulu UniAVV, byl v souvislosti s charakterem těchto dat, kdy se v provozu nevyskytla nebezpečná porucha, sestaven specifický zkušební plán předpokládající bezporuchový provoz zařízení. Vytvořený matematický model této zkoušky byl demonstrován pro případ určení intenzity poruch subsystému přenosu signálu snímače MIB.

Pro ověření parametrů bezporuchovosti elektronických systémů, tj. intenzity poruch, byl odvozen matematický model pro zrychlené zkoušky spolehlivosti soustav složených z většího počtu tvořících prvků. Tento model je založen na Arrheniově převodním vztahu pro zvýšenou teplotu zkoušky a na předpokladu exponenciálního rozdělení pravděpodobnosti dob do poruchy. Zkoušky prováděné podle tohoto programu je možné realizovat pro subsystémy jako celky, při zachování vazeb mezi jednotlivými tvořícími prvky. Pro snadné vyhodnocení výsledků zrychlených zkoušek byly vyvinuty elektronické formuláře „Arrhenius 1“, resp. „Arrhenius 2“, které umožňují výpočet parametrů bezporuchovosti v závislosti na režimu provádění zkoušek (při znalosti mechanismu vzniku poruch a jejich aktivačních energií, resp. zjednodušený přístup bez dostupných informací o aktivačních energií tvořících prvků).

Využití této disertační práce je možné také ve vysokoškolské pedagogické praxi, v rámci výuky předmětů spojených se spolehlivostí a bezpečností technických systémů. Přínos teoretické části práce představuje zejména problematika funkční bezpečnosti systémů související s bezpečností, jež je relativně nová a v tuzemských vysokoškolských učebních textech není příliš zmiňována. Přínosem pro výuku je také teorie zrychlených zkoušek spolehlivosti, která je v této práci uvedena. Experimentální část disertační práce může být využita jako případová studie aplikace principů funkční bezpečnosti. Na konkrétních příkladech z technické praxe může být objasněno použití nástrojů a postupů hodnocení spolehlivosti a bezpečnosti vycházející z požadavků normy ČSN EN 61508, případně aplikace dalších metod pro analýzu spolehlivosti (FMEA, FTA, RBD atd.).

8.2 Možnosti dalšího rozvoje problematiky

V průběhu řešení problematiky zmíněné v této práci se vyskytla řada námětů, které by mohly být dále rozvíjeny v souvislosti s analýzou spolehlivosti a funkční bezpečnosti systému automatického vedení vlaku, případně dalších technických systémů. Patří k nim mimo jiné:

- rozšíření kvalitativní analýzy rizika ze systému automatického vedení vlaku také na další systémy hnacího kolejového vozidla s vlivem na bezpečnost železniční dopravy (vozidlový počítač, zabezpečovací systém ETCS apod.), které může vést k přerozdělení požadavků funkční bezpečnosti u systémů souvisejících s bezpečností;
- uvážení provedení systému souvisejícího s bezpečností (tj. diagnostického systému) u systému automatického vedení vlaku jako systému nezávislého na jeho řídícím systému a v souvislosti s tím stanovení požadavků funkční bezpečnosti inovovaného systému;
- vytvoření teoretického modelu bezporuchovosti pro kvantitativní hodnocení spolehlivosti technických systémů, u nichž se nepředpokládá konstantní intenzita poruch, a provedení modifikace ukazatelů funkční bezpečnosti náhodných poruch hardware, které jsou normou definovány pouze pro exponenciální rozdělení pravděpodobnosti;
- další zrychlení průběhu zkoušek spolehlivosti jejich realizací při časově proměnlivém tepelném zatížení nebo při větším počtu zrychlujících zatížení (vibrace, vlhkost apod.), v této souvislosti vytvoření matematických modelů těchto zkoušek a přizpůsobení software pro vyhodnocování výsledků zkoušek.

SEZNAM POUŽITÉ LITERATURY

[1] BRIŠ, Radim. *Teorie spolehlivosti : učební text pro Fakultu aplikované informatiky, UTB Zlín* [online]. Ostrava : VŠB - TU Ostrava, 2007 [cit. 2009-11-06]. Dostupné z WWW: <http://am.vsb.cz/bris/>.

[2] BRIŠ, Radim; LITSCHMANNOVÁ, Martina. *Statistika I. pro kombinované a distanční studium* [online]. Ostrava : VŠB - TU Ostrava, 2004 [cit. 2009-11-06]. Dostupné z WWW: <http://am.vsb.cz/bris/>.

[3] DANZER, Jiří. *Elektrická trakce 9 - Řízení vozidel* [online]. Žilina : Žilinská univerzita v Žiline, 2004 [cit. 2010-03-25]. Dostupné z WWW: <http://www.kves.uniza.sk/>.

[4] FAMFULÍK, Jan; MÍKOVÁ, Jana; KRZYŽANEK, Radek. *RAMS computer - Vývoj řídícího systému pro kolejová vozidla s garantovanými parametry RAMS : Související důkaz bezpečnosti UniAVV*. Ostrava : VŠB - TU Ostrava, Institut dopravy, 2010.

[5] FAMFULÍK, Jan; MÍKOVÁ, Jana; KRZYŽANEK, Radek. *RAMS computer - Vývoj řídícího systému pro kolejová vozidla s garantovanými parametry RAMS : Technická zpráva o bezpečnosti UniAVV*. Ostrava : VŠB - TU Ostrava, Institut dopravy, 2010.

[6] FAMFULÍK, Jan; MÍKOVÁ, Jana; KRZYŽANEK, Radek. *Teorie údržby* [online]. Ostrava : VŠB - TU Ostrava, 2007 [cit. 2009-11-21]. Dostupné z WWW: <http://homel.vsb.cz/~krz011/>. ISBN 978-80-248-1509-1.

[7] HOLUB, Rudolf. *Zkoušky spolehlivosti (Stochastické metody)*. Brno : Vojenská akademie v Brně, 1992. 226 s. S-1590.

[8] HOLUB, Rudolf; VINTR, Zdeněk. *Spolehlivost letadlové techniky (elektronická učebnice)* [online]. Brno : VUT v Brně, 2001 [cit. 2009-11-21]. Dostupné z WWW: <http://lu.fme.vutbr.cz/download.php>.

[9] KECECIOGLU, Dimitri. *Reliability & Life Testing Handbook, Volume 2*. Englewood Cliffs : PTR Prentice Hall, 1994. 859 s. ISBN 0-13-772369-5.

[10] LIESKOVSKÝ, Aleš. Automatické vedení vlaků Českých drah. *Automatizace*. Říjen 2004, ročník 47, číslo 10, s. 631-632. ISSN 0005-125X.

[11] LIESKOVSKÝ, Aleš; MYSLIVEC, Ivo. *Aut. vedení vlaku AVV / Automatic train operation (ATO) AVV* [online]. 1999 [cit. 2009-04-02]. Dostupné z WWW: <http://www.volny.cz/vav3/index.htm>.

[12] LIŠKA, Petr. ERTMS - jednotný standard pro evropské železnice. *Automatizace*. Prosinec 2006, ročník 49, číslo 12, s. 786-788. ISSN 0005-125X.

[13] *Accelerated Life Testing Analysis* [online]. [cit. 2009-11-16]. Dostupné z WWW: <http://www.weibull.com/acceltestwebcontents.htm>.

[14] *Aplikace UniAVV na lokomotivě ř. 380*. Studénka: MSV elektronika s.r.o., 2008. 13 s.

[15] ČSN EN 61508-1. *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 1: Všeobecné požadavky.* Praha : Český normalizační institut, 2002. 60 s.

[16] ČSN EN 61508-2. *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností.* Praha : Český normalizační institut, 2002. 76 s.

[17] ČSN EN 61508-4. *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 4: Definice a zkratky.* Praha : Český normalizační institut, 2002. 32 s.

[18] ČSN EN 61508-5. *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 5: Příklady metod určování úrovní integrity bezpečnosti.* Praha : Český normalizační institut, 2002. 32 s.

[19] ČSN EN 61508-6. *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností - Část 6: Metodické pokyny pro použití IEC 61508-2 a IEC 61508-3.* Praha : Český normalizační institut, 2002. 72 s.

[20] *Life Data Analysis (Weibull Analysis)* [online]. Confidence Bounds for the Exponential Distribution [cit. 2010-04-28]. Dostupné z WWW: <http://www.weibull.com/lifedatawebcontents.htm>.

[21] MIL-HDBK-217F. *Reliability Prediction of Electronic Equipment*. Washington DC : Department of Defense, 1991. 205 p.

[22] *ReliaSoft's Xfmea Version 4 : Software Training Guide* [online]. Tucson : ReliaSoft Corporation, 2006 [cit. 2010-04-02]. Dostupné z WWW: <http://Xfmea.ReliaSoft.com>.

[23] MYSLIVEC, Ivo - ústní sdělení (AŽD Praha s.r.o., Žirovnická 2, Praha 10) dne 9. září 2009

SEZNAM VLASTNÍCH PUBLIKACÍ DOKTORANDA

Publikace vztahující se k tématu disertační práce

FAMFULÍK, Jan; MÍKOVÁ, Jana; KRZYŽANEK, Radek. *Teorie údržby* [online]. Ostrava : VŠB - TU Ostrava, 2007. Dostupné z WWW: <http://homel.vsb.cz/~krz011/>. ISBN 978-80-248-1509-1.

KRZYŽANEK, Radek; FAMFULÍK, Jan. Stanovení požadavků na spolehlivost při dílčí modernizaci lokomotiv. In *Sborník konference „Opotřebení, spolehlivost, diagnostika 2007“, Brno 30. – 31. října 2007.* Ed. Jiří Šťastný. Brno: Univerzita obrany, 2007, s. 163 – 168. ISBN 978-80-7231-294-8.

FAMFULÍK, Jan; KRZYŽANEK, Radek. Určení parametrů spolehlivosti návěstního světla na bázi LED. *Nová železniční technika*, srpen 2008, roč. 16, č. 4, s. 30 – 33. ISSN 1210-3942.

FAMFULÍK, Jan; KRZYŽANEK, Radek. Functional Safety Assessment of LED Based Signal Lamp. *Mechanics Transport Communications* [online]. 2009, is. 1. Dostupný z WWW: <http://www.mtc-aj.com/>. ISSN 1312-3823.

FAMFULÍK, Jan; MÍKOVÁ, Jana; KRZYŽANEK, Radek. Mission completion probability of cycle rate system. In BRIŠ, GUEDES SOARES, MARTORELL (eds), *Reliability, Risk and Safety : Theory and Applications*. London : Taylor & Francis Group, 2010. s. 1603-1606. ISBN 978-0-415-55505-8.

FAMFULÍK, Jan; KRZYŽANEK, Radek; GALVAS, Peter. *Zkoušky spolehlivosti (vybrané stochastické metody)*. Ostrava : VŠB - Technická univerzita Ostrava, 2010. 67 s. ISBN 978-80-248-2278-8.

Ostatní publikace

FAMFULÍK, Jan; KRZYŽANEK, Radek. Sestavení programu preventivní údržby s využitím metodiky RCM. *Zdvihací zařízení v teorii a praxi*, 2007, č. 2, s. 2 – 7. Dostupný z WWW: <http://www.id.vsb.cz/zdvihacizarizeni/default.htm>. ISSN 1802-2812.

FAMFULÍK, Jan; KRZYŽANEK, Radek. Stanovení intervalů preventivní údržby při údržbě RCM. *Zdvihací zařízení v teorii a praxi*, 2007, č. 2, s. 8 – 11. Dostupný z WWW: <http://www.id.vsb.cz/zdvihacizarizeni/default.htm>. ISSN 1802-2812.

KRZYŽANEK, Radek. RCM Method Utilization for Tramcar Maintenance. *Mechanics Transport Communications* [online]. 2010, is. 1. Dostupný z WWW: <http://www.mtc-aj.com/>. ISSN 1312-3823.

SEZNAM OBRÁZKŮ

Obr. č. 1.1: Schéma analýzy spolehlivosti modulu UniAVV 13
Obr. č. 2.1: Blokové schéma funkcí systému AVV 15
Obr. č. 2.2: Ilustrace funkcí AVV – vznik nebezpečné události 17
Obr. č. 2.3: Blokové schéma systému AVV 19
Obr. č. 2.4: Principiální schéma systému ERTMS/ETCS 24
Obr. č. 3.1: Životní cyklus celkové bezpečnosti 26
Obr. č. 3.2: Životní cyklus hardware E/E/PE systémů 27
Obr. č. 3.3: Sériové uspořádání subsystémů 30
Obr. č. 3.4: Paralelní uspořádání subsystémů 30
Obr. č. 3.5: Princip nutného snížení rizika 31
Obr. č. 3.6: Koncepce metody ALARP 32
Obr. č. 3.7: Diagram rizika, určení úrovně integrity bezpečnosti (SIL) 35
Obr. č. 3.8: Architektura 1oo1 39
Obr. č. 3.9: Pomyslné blokové schéma subsystému 1oo1 40
Obr. č. 3.10: Architektura 1oo2 41
Obr. č. 3.11: Architektura 2oo2 42
Obr. č. 3.12: Architektura 1oo2D 42
Obr. č. 4.1: Znázornění zkušebních plánů: r – plány 44
Obr. č. 4.2: Znázornění zkušebních plánů: t – plány 45
Obr. č. 4.3: Úrovně zatížení výrobku 47
Obr. č. 4.4: Průběh hustoty pravděpodobnosti pro provozní a zvýšené zatížení 48
Obr. č. 4.5: Arrheniův model – závislost parametru spolehlivosti na teplotě 50
Obr. č. 4.6 Schéma zkoušky, blokový diagram bezporuchovosti systému 51
Obr. č. 4.7: Schéma zkoušky, blokový diagram bezporuchovosti systému 53
Obr. č. 5.1: Matice RPN x Závažnost 64
Obr. č. 5.2: Příklad přiřazení úrovně integrity bezpečnosti (SIL) 69
Obr. č. 5.3: Přiřazení požadavků SIL subsystémům AVV 71
Obr. č. 5.4: Analýza FMEA – srovnání Risk Priority Number 75
Obr. č. 6.1: Strom poruch systému AVV, obecný přístup 83
Obr. č. 6.2: Strom poruch systému AVV, skutečný stav 85
Obr. č. 6.3: Pravděpodobnost $F_{DU}(t)$ systému AVV, srovnání rozdílných SIL 88
Obr. č. 6.4: Interval pravděpodobnosti $F_{DU}(t)$ systému AVV podle požadavků na SIL 89
Obr. č. 6.5: Strom poruch, modul UniAVV 90
Obr. č. 6.6: Pravděpodobnost $F_{DU}(t)$, $F_{DD}(t)$ pro různé diagnostické pokrytí 92
Obr. č. 6.7: Blokové schéma modulu UniAVV s požadavky na SIL 93
Obr. č. 6.8: Blokové schéma bloku logiky modulu UniAVV 94
Obr. č. 6.9: Dekompozice modulu UniAVV pro určení intenzit poruch 97
Obr. č. 6.10: Blok logiky, pravděpodobnost poruchy $F_{DD}(t)$, $F_{DU}(t)$ 101
Obr. č. 7.1: Schéma zkušebního t-plánu pro $r = 0$ poruch 108
Obr. č. 7.2: Akumulovaná doba zkoušky pro prokázání SIL v závislosti na DC 111
Obr. č. 7.3: Zkušební plán pro zkoušku typu „Arrhenius 1“ 116
Obr. č. 7.4: Příklad zadávaných údajů pro zrychlenou zkoušku 117
Obr. č. 7.5: Příklad zadávání údajů o poruchách výrobků 117

Obr. č. 7.6: Příklad vyhodnocení zrychlené zkoušky 118
Obr. č. 7.7: Zkušební plán pro dílčí zkoušku typu „Arrhenius 2“ 120
Obr. č. 7.8: Příklad zadávaných údajů pro zrychlenou zkoušku 121
Obr. č. 7.9: Příklad zadávání údajů o poruchách výrobků 121
Obr. č. 7.10: Příklad vyhodnocení zrychlené zkoušky 122
Obr. č. 7.11: Vývojový diagram formuláře „Arrhenius 1“ 124
Obr. č. 7.12: Vývojový diagram formuláře „Arrhenius 2“ 125
Obr. č. 7.13: Závislost akumulované pracovní doby na intenzitě poruch 127

SEZNAM TABULEK

Tabulka č. 3.1: Cílová míra poruch pro úrovně integrity bezpečnosti v režimu provozu s nízkým vyžádáním 29
Tabulka č. 3.2: Cílová míra poruch pro úrovně integrity bezpečnosti v režimu provozu s vysokým nebo nepřetržitým vyžádáním 29
Tabulka č. 3.3: Klasifikace rizika, obecný případ 33
Tabulka č. 3.4: Následek nebezpečné události 34
Tabulka č. 3.5: Režim vyžádání funkce 34
Tabulka č. 3.6: Možnost se vyhnout nebezpečné události 34
Tabulka č. 3.7: Pravděpodobnost nežádoucího výskytu 35
Tabulka č. 3.8: Omezení architektury hardware v souvislosti s integritou bezpečnosti 37
Tabulka č. 5.1: Klasifikace závažnosti poruchy (ES) 58
Tabulka č. 5.2: Klasifikace četnosti poruchy (CO) 58
Tabulka č. 5.3: Klasifikace odhalitelnosti poruchy (CD) 59
Tabulka č. 5.4: Seznam příčin poruch systému AVV 60
Tabulka č. 5.5: Analýza FMEA – modul CRV 61
Tabulka č. 5.6: Analýza FMEA – moduly RCB a OJV 63
Tabulka č. 5.7: Funkce modulu UniAVV – nutnost opatření ke snížení rizika 65
Tabulka č. 5.8: Příklad klasifikace parametrů rizika funkce modulu UniAVV 68
Tabulka č. 5.9: Přiřazení parametrů rizika a úrovní integrity bezpečnosti (SIL) 70
Tabulka č. 5.10: Omezení architektury modulu UniAVV, systém bez zálohování 73
Tabulka č. 5.11: Omezení architektury modulu UniAVV, systém se zálohováním 73
Tabulka č. 5.12: Analýza FMEA (po opatření) – modul CRV 76
Tabulka č. 5.13: Analýza FMEA (po opatření) – moduly RCB a OJV 78
Tabulka č. 6.1: Požadavky parametrů funkční bezpečnosti 95
Tabulka č. 6.2: Diagnostické pokrytí prvku, složky intenzit poruch – výřez 98
Tabulka č. 6.3: Intenzity poruch, poměr bezpečných poruch bloku logiky 99
Tabulka č. 6.4: Porovnání dosažených výsledků 103
Tabulka č. 7.1: Snímače MIB, akumulovaná pracovní doba zkoušky 107
Tabulka č. 7.2: Aktivační energie mechanismů poruch elektronických prvků 115